Analisis Dampak Serangan *Black Hole* terhadap Kinerja Protokol AODV dan DYMO pada MANET (*Mobile Ad-Hoc Network*)

SKRIPSI

Untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun oleh:
I Putu Krisna Yoga Tanaya
NIM: 145150201111109

PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2018

PENGESAHAN

Analisis Dampak Serangan *Black Hole* terhadap Kinerja Protokol AODV dan DYMO pada MANET (*Mobile Ad-Hoc Network*)

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun Oleh :
Nama: I Putu Krisna Yoga Tanaya
NIM: 145150201111109

Skripsi ini telah diuji dan dinyatakan lulus pada

26 Desember 2018

Telah diperiksa dan disetujui oleh:

Dosen Pembimbing I	Dosen Pembimbing II
Rakhmadhany Primananda, S.T, M.Kom	Ir. Heru Nurwarsito, M.Kom
NIK. 2016098604061001	NIP. 196504021990021001

Mengetahui
Ketua Jurusan Teknik Informatika

Tri Astoto Kurniawan, S.T, M.T, Ph.D
NIP. 19710518 200312 1 001

PERNYATAAN ORISINALITAS

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis disitasi dalam naskah ini dan disebutkan dalam daftar pustaka.

Apabila ternyata didalam naskah skripsi ini dapat dibuktikan terdapat unsur-unsur plagiasi, saya bersedia skripsi ini digugurkan dan gelar akademik yang telah saya peroleh (sarjana) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).

Malang, 26 Desember 2018

I Putu Krisna Yoga Tanaya

NIM: 145150201111109

PRAKATA

Segala puji dan syukur kepada Tuhan Yang Maha Esa yang telah memberikan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul "Analisis Dampak Serangan *Black Hole* terhadap Kinerja Protokol AODV dan DYMO pada MANET (*Mobile Ad-Hoc Network*)".

Dengan selesainya skripsi ini, penulis mengucapkan terimakasih kepada pihak-pihak yang telah membantu penulis selama penyusunan skripsi, diantaranya:

1. Ida Sang Hyang Widhi Wasa yang telah memberi kemudahan dalam semua proses penulisan skripsi ini.
2. Kedua orang tua penulis, yaitu I Made Dwi Sutanegara, S.E dan Ni Putu Deni Trisnawati, S.E. Kedua adik kandung penulis yaitu Ni Made Febby Dwi Paramitha dan Ni Nyoman Fanny Cantika Putri beserta keluarga besar yang selalu memberikan do'a, motivasi, dan semangat dalam proses penyelesaian skripsi ini.
3. Bapak Rakhmadhany Primananda, S.T, M.Kom selaku dosen pembimbing I yang telah meluangkan waktu untuk memberikan masukan, ilmu, serta saran yang bermanfaat dalam proses penyelesaian skripsi ini.
4. Bapak Ir. Heru Nurwarsito, M.Kom selaku dosen pembimbing II yang telah meluangkan waktu untuk memberikan masukan, ilmu, serta saran yang bermanfaat dalam proses penyelesaian skripsi ini.
5. Bapak Wayan Firdaus Mahmudy, S.Si, M.T, Ph.D, Bapak Ir. Heru Nurwasito, M.Kom, Bapak Drs. Mardji, M.T, dan Bapak Edy Santoso, S.Si, M.Kom selaku Dekan, Wakil Dekan 1, Wakil Dekan 2, dan Wakil Dekan 3 Fakultas Ilmu Komputer, Universitas Brawijaya.
6. Bapak Tri Astoto Kurniawan, S.T, M.T, Ph.D dan Bapak Agus Wahyu Widowo, S.T, M.Cs selaku Ketua Jurusan Teknik Informatika dan Kepala Program Studi Teknik Informatika Fakultas Ilmu Komputer, Universitas Brawijaya.
7. Sahabat-sahabat #nyame yang selalu mendukung dalam pembuatan penelitian ini.
8. Sahabat-sahabat seperjuangan geng manet (Ilin, Imam, Atem, Asroful, Eko, Alif, Ode) yang bersedia mendukung dan membantu dalam penyelesaian skripsi ini.
9. Kekasih hati penulis Kadek Chintya Nurlita Widyahastuti yang selalu memberikan dukungan dan kasih saying, menjadi penghibur serta pengingat bagi penulis untuk tidak bermalas-malasan dan tempat berkeluh kesah dalam penyelesaian skripsi ini.

10. Seluruh Dosen Fakultas Ilmu Komputer, Universitas Brawijaya atas kesediaannya dalam mengajarkan dan membagikan ilmu yang bermanfaat bagi penulis.
11. Semua pihak yang turut berperan dalam penyelesaian skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna. Oleh karna itu, penulis mengharapkan kritik dan saran yang bersifat membangun. Semoga skripsi ini nantinya dapat bermanfaat dan memberikan sumbangan yang berarti bagi pihak yang membutuhkan.

Malang, 26 Desember 2018

Penulis

krisnayoga96@gmail.com

ABSTRAK

I Putu Krisna Yoga Tanaya, Analisis Dampak Serangan *Black Hole* terhadap Kinerja Protokol AODV dan DYMO pada MANET (*Mobile Ad-Hoc Network*)

Pembimbing: Rakhmadhany Primananda, S.T, M.Kom dan Ir. Heru Nurwarsito, M.Kom

Mobile Ad-Hoc Network (MANET) merupakan sekumpulan perangkat *mobile* yang saling berkomunikasi melalui jaringan nirkabel tanpa adanya jaringan terpusat atau terstruktur. Pada MANET terdapat tiga jenis protokol *routing* yaitu protokol *routing* proaktif, protokol *routing* reaktif, dan protokol *routing* hibrida. Salah satu karakteristik khusus pada MANET yaitu keterbatasan keamanan menyebabkan segi keamanan menjadi kelemahan pada MANET sehingga serangan-serangan yang terdapat pada MANET dapat menyebabkan penurunan kinerja pada protokol *routing*. Bedasarkan permasalahan tersebut, maka penulis membuat penelitian yang berjudul Analisis Dampak Serangan *Black Hole* terhadap Kinerja Protokol AODV dan DYMO pada MANET (*Mobile Ad-Hoc Network*). Hasil yang diperoleh dalam penelitian ini yaitu serangan *black hole* berdampak terhadap kinerja protokol AODV dan protokol DYMO. Pengujian dilakukan menggunakan *network simulator-2* (*NS-2*) dengan tiga skenario pengujian, yaitu kepadatan 40, 60, dan 80 *node* dengan variasi jumlah *node* penyerang (*black hole*). Variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, dan 20. Parameter kinerja yang digunakan dalam pengujian meliputi *packet delivery ratio*, *normalized routing load*, dan *packet loss*. Hasil penelitian menunjukan bahwa *packet delivery ratio* protokol DYMO lebih baik dari protokol AODV dengan rata-rata keseluruhan hasil PDR pada protokol AODV sebesar 34,2%. Sedangkan pada protokol DYMO sebesar 42,1%.

Kata kunci: MANET, AODV, DYMO, *black hole, NS-2, packet delivery ratio, normalized routing load, packet loss*

ABSTRACT

I Putu Krisna Yoga Tanaya, ***Analysis Impact of Black Hole Attacks on the Performance of AODV and DYMO Protocols on MANET (Mobile Ad-Hoc Network)***

***Supervisors*: Rakhmadhany Primananda, S.T, M.Kom dan Ir. Heru Nurwarsito, M.Kom**

Mobile Ad-Hoc Network (MANET) is a set of mobile devices that communicates with each other over wireless networks without a centralized or structured network. MANET has three types of routing protocols, it named proactive routing protocol, reactive routing protocol, and hybrid routing protocol. One particular characteristic of MANET, which is security limitations, causes security to be a weakness in MANET so that attacks on MANET can cause a decrease in performance in the routing protocol. Based on these problems, the authors made a study entitled Analysis Impact of Black Hole Attacks on the Performance of AODV and DYMO Protocols on MANET (Mobile Ad-Hoc Network). The result in this study is black hole attacks affected the performance of the AODV protocol and the DYMO protocol. Tests are carried out using network simulator-2 (NS-2) with three test scenarios, those are a density of 40, 60, and 80 nodes with variations in the number of attack nodes (black holes). Variation in the number of attack nodes (black holes) as many as 5, 10, 15, and 20. Performance parameters that used in this test is including the packet of delivery ratio, normalized routing load, and packet loss. The results of the study show that the packet delivery ratio on the DYMO protocol is better than the AODV protocol with an average overall PDR *result in the AODV protocol of 34,2%. While the DYMO protocol is 42,1%.*

Keywords: MANET, AODV, DYMO, black hole, NS-2, packet delivery ratio, normalized routing load, packet loss

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1 PENDAHULUAN

1.1 Latar belakang

MANET atau *Mobile Ad-Hoc Network* merupakan sekumpulan perangkat *mobile* yang saling berkomunikasi melalui jaringan nirkabel tanpa adanya jaringan terpusat atau terstruktur. Perangkat *mobile* pada MANET disebut sebagai *node* yang dapat berguna sebagai pengirim atau penerima data dan *node* juga dapat berguna sebagai penghubung *node* lain. Sehingga untuk mengatur seluruh proses *routing* pada *topologi* MANET tidak memerlukan *router*, karena pada setiap *node* dapat berfungsi sebagai *router* untuk menentukan arah tujuan yang akan ditentukan (Amillia, 2014).

Pada MANET terdapat tiga jenis protokol *routing* yaitu protokol *routing* proaktif, protokol *routing* reaktif, dan protokol *routing* hibrida. Protokol *routing* yang akan dibahas dalam penelitian ini termasuk dalam jenis protokol *routing* reaktif yaitu protokol *Ad hoc On-Demand Distance Vector (*AODV*)* dan *Dynamic Mobile Ad-Hoc Network On-demand* (DYMO*),* dimana pada protokol *routing* reaktif *node-node* akan mencari jalur ke tujuan ketika dibutuhkan. Protokol AODV dan DYMO dipilih penulis karena kedua protokol tersebut termasuk dalam satu jenis protokol *routing* yaitu reaktif *routing* dan protokol DYMO merupakan protokol penerus dari protokol AODV yang sudah populer pada MANET. Kelebihan pada protokol DYMO yaitu mampu untuk mengetahui informasi tentang semua *node* antara *node* sumber dan *node* tujuan di jalur yang baru, sedangkan protokol AODV hanya mengetahui informasi *node* sumber dan *node* tujuan (Anshori, 2013).

MANET memiliki beberapa karakteristik khusus seperti topologi yang dinamis, algoritma yang sederhana, dan keterbatasan keamanan (Ardiyansyah, 2016), sehingga segi keamanan dapat dinyatakan salah satu kelemahan pada MANET. Secara umum serangan-serangan yang dilakukan pada MANET bertujuan untuk mengetahui informasi yang dikirimkan antar *node* dengan cara menyusup diantara *node-node* yang ada pada jaringan ataupun dengan cara membanjiri jaringan dengan *node-node* jahat (Harahap, 2014). Salah satu serangan yang terdapat pada MANET yaitu serangan *black hole.* Serangan *black hole* merupakan serangan pada jaringan MANET mengakibatkan paket-paket yang melewati *node black hole* tersebut akan di-*drop* dan akan menyebabkan paket tersebut hilang (Shukla, 2014).

Berdasarkan penelitian yang dilakukan oleh Andi Yusuf Hadi Wibowo yang berjudul "Analisis Kinerja *Routing Protocol Ad Hoc On Demand Distance Vector* Terhadap Serangan *black hole* Pada *Mobile Ad Hoc Network*" membahas tentang kinerja protokol *routing* sebelum dan sesudah terjadi serangan *black hole* dari faktor jumlah *node* pada suatu jaringan dan dari ukuran paket data. Richa Agrawal yang berjudul "*Performance Comparison of* AODV *and* DYMO MANET *Protocols under Wormhole Attack Environment*" membahas tentang perbandingan kinerja protokol AODV dan DYMO terhadap serangan *wormhole* dari faktor jumlah *node* pada suatu jaringan dan dari pengaruh kecepatan mobilitas *node* terhadap

parameter *packet loss, average end-to-end delay, dan throughput* (Agrawal, 2012). Pada penelitian tersebut tidak disampaikan tentang jumlah variasi *node* penyerang.

Dalam penelitian ini penulis membuat penelitian dengan membandingkan kinerja pada protokol AODV dan protokol DYMO terhadap serangan *black hole.* Pengujian dilakukan menggunakan *network simulator-2* dengan tiga skenario pengujian, yaitu kepadatan 40 *node* dengan variasi jumlah *node* penyerang (*black hole*), kepadatan 60 *node* dengan variasi jumlah *node* penyerang (*black hole*), dan kepadatan 80 *node* dengan variasi jumlah *node* penyerang (*black hole*). Parameter kinerja yang digunakan dalam pengujian meliputi *packet delivery ratio, normalized routing load,* dan *packet loss*.

1.2 Hipotesis Penelitian

Berdasarkan latar belakang yang telah dipaparkan, maka peneliti memiliki hipotesis bahwa protokol DYMO akan memiliki kinerja lebih baik dibandingkan protokol AODV, karena protokol DYMO merupakan penerus dari protokol *routing* AODV dan menurut teori protokol DYMO memiliki kemampuan untuk mengetahui informasi tentang semua *node* antara *node* sumber dan *node* tujuan di jalur yang baru. Sedangkan AODV hanya mengetahui informasi *node* sumber dan *node* tujuan.

1.3 Rumusan Masalah

Berdasarkan penjabaran pada latar belakang, maka dapat dirumuskan permasalahan sebagai berikut:

1. Bagaimana implementasi serangan *black hole* pada protokol AODV dan protokol DYMO pada MANET?
2. Bagaimana dampak serangan *black hole* terhadap kinerja protokol AODV dan protokol DYMO pada pengaruh kepadatan jumlah *node* dengan variasi banyak *node* penyerang (*black hole*)?
3. Bagaimana parameter kinerja *packet delivery ratio, normalized routing load,* dan *packet loss* terhadap kinerja protokol AODV dan protokol DYMO?

1.4 Tujuan

Tujuan yang ingin dicapai oleh penulis pada penelitian ini adalah sebagai berikut:

1. Mengetahui implementasi serangan *black hole* pada protokol AODV dan protokol DYMO.
2. Mengetahui dampak serangan *black hole* terhadap kinerja protokol AODV dan protokol DYMO pada pengaruh kepadatan jumlah *node* dengan variasi banyak *node* penyerang (*black hole*).

3. Mengetahui parameter kinerja *packet delivery ratio, normalized routing load,* dan *packet loss* terhadap kinerja protokol AODV dan protokol DYMO.

1.5 Manfaat

Manfaat dari penelitian ini adalah sebagai berikut :

1. Mampu memperkaya teori-teori yang sudah ada dan dapat mengembangkan teori-teori yang sedang berkembang.
2. Mampu memberikan referensi mengenai perbandingan kinerja antara protokol AODV dan protokol DYMO saat terjadi serangan *black hole* dengan variasi banyak *node* penyerang.

1.6 Batasan masalah

Batasan masalah yang digunakan dalam penelitian ini antara lain sebagai berikut :

1. Protokol *routing* yang digunakan adalah protokol AODV dan protokol DYMO.
2. Jenis serangan yang digunakan adalah serangan *black hole* yang bersifat internal.
3. Skenario pengujian yang dilakukan yaitu pengujian kepadatan *node* dengan variasi jumlah *node* penyerang (*black hole*).
4. Kepadatan jumlah *node* yang digunakan dalam simulasi sebanyak 40, 60, dan 80 *node*.
5. Variasi jumlah *node* penyerang (*black hole*) yang digunakan dalam simulasi sebanyak 5, 10, 15, dan 20.
6. Parameter yang digunakan untuk menganalisa hasil yaitu *packet delivery ratio, normalized routing load,* dan *packet loss*.
7. Penelitian ini di implementasikan menggunakan *network simulator-2*.
8. Penelitian ini hanya membandingkan kinerja protokol yang terbaik pada serangan *black hole* di protokol AODV dan DYMO.

1.7 Sistematika pembahasan

Sistematika penulisan dalam penelitian ini sebagai berikut :

Bab I: Pendahuluan

Pada bab ini berisikan deskripsi dari latar belakang, tujuan, manfaat, batasan masalah, sistematika penulisan, dan jadwal pengerjaan dari penelitian.

Bab II: Landasan Kepustakaan

Pada bab ini berisikan deskripsi dari dasar teori dan referensi yang mendasari penelitian, teknologi MANET dan protokol *routing* yang digunakan dalam simulasi.

Bab III: Metodologi Penelitian

Pada bab ini berisikan deskripsi dari langkah-langkah yang dilakukan dalam melakukan penelitian terdiri dari landasan kepustakaan, implementasi, pengujian, hasil dan pembahasan serta pengambilan kesimpulan.

Bab IV: Perancangan dan Implementasi

Pada bab ini berisikan tentang pemaparan dari perancangan skenario simulasi, parameter kinerja, serta serangan *black hole* dan dilakukan implementasi sesuai pemaparan pada perancangan sistem.

Bab V: Pengujian dan Analisis

Pada bab ini berisikan pengujian dan analisis yang dilakukan terhadap sistem yang telah direalisasikan pada implementasi.

Bab VI: Penutup

Pada bab ini berisikan deskripsi dari kesimpulan dan saran berdasarkan hasil dan analisis penelitian.

BAB 2 LANDASAN KEPUSTAKAAN

Pada bab ini berisi kajian pustakan dan dasar teori yang terkait dengan penelitian yang akan dilakukan. Kajian pustakan yang akan digunakan didasari oleh penelitian terdahulu terkait dengan protokol AODV dan protokol DYMO pada MANET.

2.1 Kajian Pustaka

Dalam penelitian ini dicantumkan penelitian terkait agar dijadikan pertimbangan dan studi literatur pada pengerjaan penelitian. Berikut adalah tabel perbandingan terdahulu dengan penelitian yang akan dilakukan:

Tabel 2.1 Kajian Pustaka

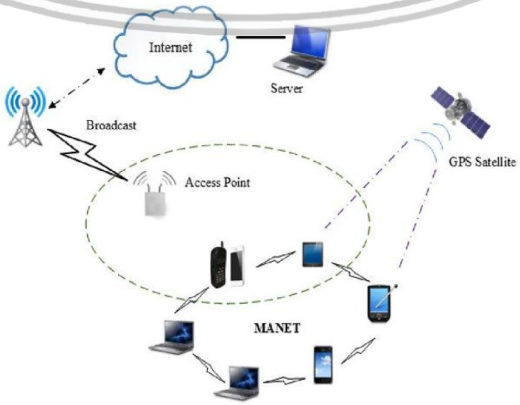
No	Nama peneliti, tahun, judul	Persamaan	Perbedaan	
			Penelitian terdahulu	Rencana penelitian
1	Andi Yusuf Hadi Wibowo, 2015, Analisis Kinerja *Routing Protocol Ad Hoc On Demand Distance Vector* Terhadap Serangan *black hole* Pada *Mobile Ad Hoc Network*	Mengunakan protokol *routing* AODV, terdapat serangan *black hole* pada protokol *routing* AODV, di implementasikan pada jaringan MANET menggunakan *NS-2*	Jumlah *node* 10, 20, dan 30. Serangan *black hole* hanya berasal dari satu *node*. Parameter yang digunakan adalah *end to end delay, packet delivery ratio, throughput*, dan *routing overhead*	Jumlah *node* 40, 60, dan 80. Terdapat variasi jumlah *node* penyerang (*black hole*). Parameter yang digunakan adalah *packet delivery ratio, normalized routing load,* dan *packet loss*.
2	Richa Agrawal, 2012, *Performance Comparison of* AODV *and* DYMO MANET *Protocols under Wormhole Attack Environment*	Menggunakan protokol *routing* AODV dan DYMO, di implementasikan pada jaringan MANET	Di implementasikan menggunaan *QualNet version 5*. Menggunakan serangan *Wormhole* pada protokol AODV dan DYMO.	Di implementasikan menggunakan *NS-2.* Menggunakan serangan *black hole* pada protokol AODV dan DYMO dengan variasi

			Parameter yang digunakan adalah *packet loss, end to end delay,* dan *throughput.*	jumlah *node* penyerang. Parameter yang digunakan adalah *packet delivery ratio, normalized routing load,* dan *packet loss*.

2.2 *Mobile Ad-Hoc Network* (MANET)

Mobile Ad-Hoc Network (MANET) merupakan sebuah jaringan nirkabel tanpa infrastruktur yang tetap *(less infrastructure)* sehingga *node* setiap saat dapat meninggalkan atau bergabung dengan jaringan. *Node* bisa berperan sebagai *host* atau *router*. Tanpa kendali otoritas yang terpusat, komunikasi terjadi diantara *node-node*, dimana masing-masing *node* mentransmisikan paket secara independen dengan mengevaluasi *node-node* yang terdekat (Deka & Khaturia, 2014). Berikut merupakan keuntungan dan karakteristik dari MANET (Sakalabattula & Kumar, 2017) :

1. Keuntungan utama menggunakan MANET yaitu *router* bebas mengakses internet tanpa adanya *router nirkabel*. Karena itu, menggunakan MANET dapat lebih terjangkau daripada menggunakan jaringan pada umumnya.
2. Terdapat toleransi kesalahan jika terdapat kegagalan koneksi, karena pada protokol *routing* MANET dirancang untuk mengatasi kesalahan tersebut.
3. *Node-node* pada jaringan MANET dapat mengatur dirinya sendiri secara dinamis pada topologi jaringan yang berubah-ubah.

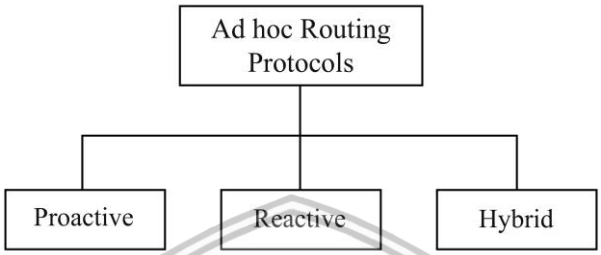


Gambar 2.1 *Mobile Ad-Hoc Network*

Sumber : (Sakalabattula & Kumar, 2017)

2.3 Protokol *Routing* pada MANET

Protokol *routing* mengatur *routing* dari paket pada MANET. Pada MANET, setiap *node* yang ada tidak mengetahui topologi dari jaringan sehingga dibutuhkan mekanisme pencarian topologi. Protokol *routing* MANET dapat dibagi menjadi tiga kategori yaitu protokol *routing* proaktif *(table driven)*, protokol *routing* reaktif *(on-demand)*, dan protokol *routing* hibrida (Rohal, et al., 2013).



Gambar 2.2 Protokol *Routing* MANET

Sumber : (Jamal, n.d.)

2.3.1 Protokol *Routing* Reaktif

Protokol *routing* reaktif pada MANET biasa juga disebut dengan protokol *routing on demand*. Terdapat dua fungsi utama pada protokol *routing* reaktif yaitu *route discovery* dan *route maintenance*. *Route discovery* berfungsi sebagai menemukan jalur ke *node* tujuan pada rute yang baru, sedangkan *route maintenance* berfungsi untuk mendeteksi jalur yang rusak dan memperbaiki rute yang telah ada sehingga pesan dapat sampai *node* tujuan. Seperti sebutannya yaitu *on demand*, yang berarti protokol *routing* ini tidak memiliki tabel *routing* yang permanen sehingga rute akan dibentuk jika diinginkan oleh *node* sumber (Chavan, 2016).

2.3.1.1 Protokol AODV (Ad Hoc On-demand Distance Vector)

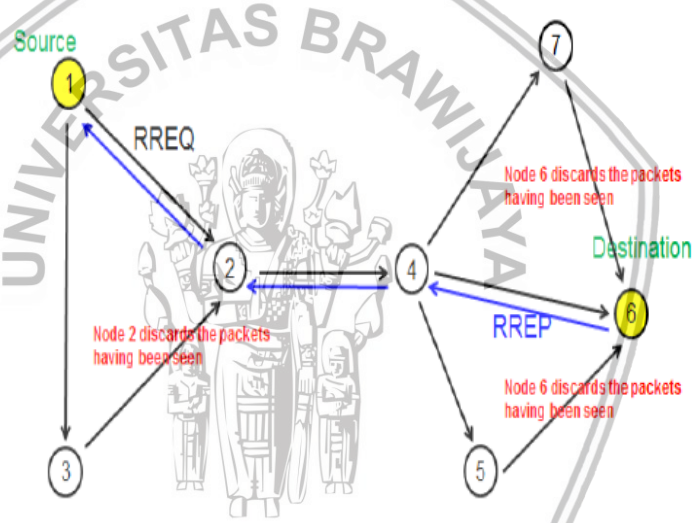
*Ad hoc On-Demand Distance Vector (*AODV*) Routing* adalah protokol *routing* untuk jaringan *ad hoc mobile (*MANETs*)* dan jaringan *ad-hoc* nirkabel lainnya. Ini dikembangkan bersama di *Nokia Research Center*, Universitas California, Santa Barbara dan Universitas Cincinnati oleh C. Perkins, E. Belding-Royer dan S. Das. AODV mampu melakukan *routing unicast* dan *multicast*. AODV adalah protokol *routing* reaktif, yang berarti menetapkan rute ke tujuan hanya sesuai permintaan. Sebaliknya, protokol *routing* internet yang paling umum bersifat proaktif, yang berarti mereka menemukan jalur *routing* secara independen dari penggunaan jalur. AODV, seperti namanya, sebuah protokol *routing distance-vector*. AODV menghindari masalah *count-to-infinity* dari protokol *distance-vector* lainnya dengan menggunakan *sequence number* pada *update* rute, sebuah teknik yang dipelopori oleh DSDV. Di AODV, jaringan diam sampai koneksi diperlukan. Pada intinya *node* membutuhkan permintaan untuk melakukan koneksi (Lee, 2011).

Berikut merupakan proses *route discovery* dan *route maintenance* pada protokol AODV (Kaur, 2014):

1. AODV *Route Discovery*

   Pada proses *route discovery*, ketika *node* ingin berkomunikasi dengan *node* lainnya, hal pertama yang dilakukan yaitu dengan melihat tabel *routing* dan jika terdapat rute menuju ke *node* tujuan maka pesan akan dikirim ke *node* tujuan, jika tidak ditemukan rute menuju tujuan maka *node* sumber akan mengirimkan pesan RREQ pada *node* tetangganya.

   Node 1 merupakan *node* sumber mengirimkan pesan RREQ pada tetangga terdekat yaitu *node* 2 dan *node* 3. *Node* 2 dan *node* 3 menerima pesan RREQ dan akan mengirimkan pesan RREQ pada *node* tetangga terdekat juga sehingga pesan RREQ sampai pada *node* 6 yaitu *node* tujuan.



Gambar 2.3 AODV *Route Discovery*

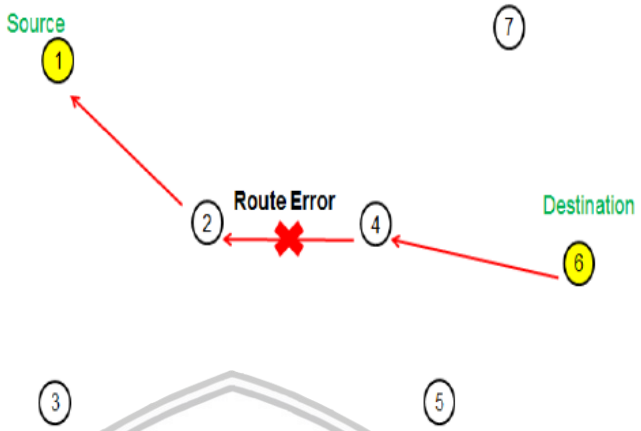
Sumber : (Kaur, 2014)

   Ketika *node* 6 (tujuan) yaitu *node* tujuan menerima pesan RREQ maka pesan RREP akan dikirimlah kembali ke *node* yang mengirimkan pesan RREQ sehingga sampai pada *node* 1 (sumber). Ketika pesan RREP mencapai *node* 1 (sumber), maka rute menuju *node* tujuan akan terbentuk dan *node* 1 (sumber) dapat berkomunikasi dengan *node* 6 (tujuan).

2. AODV *Route Maintenance*

   Terbentuknya rute pada AODV dengan memanfaatkan pesan hello untuk mendeteksi *node* tetangga terdapat dalam jangkauan atau tidak. Ketika *node* terdeteksi terputus dalam rute yang aktif, maka pesan *error* RERR akan dibuat *node* tersebut dan mengirimkan pesan *error* RERR terhadap *node-node* secara *multicast* yang memiliki hubungan dengan rute tersebut. Setelah menerima pesan *error* RERR

tersebut, *node* akan memperbaharui tabel *routing* masing-masing dan menghapus rute tersebut.



Gambar 2.4 AODV *Route Maintenance*

Sumber : (Kaur, 2014)

Jalur dari *node* 6 (tujuan) ke *node* 4 terputus, lalu pesan *error* akan dikirim ke *node* 1 (sumber), rute sebelumnya akan dihapus pada tabel *routing* dan akan dilakukan pencarian rute kembali.

2.3.1.2 Protokol DYMO (Dynamic *Mobile Ad-Hoc Network* On-demand)

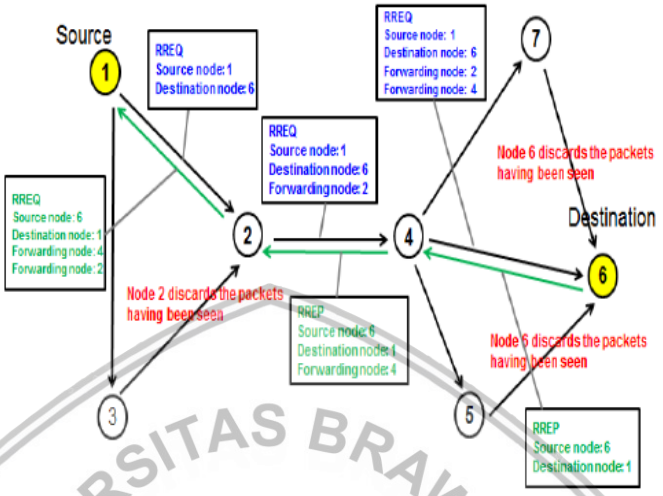
Dynamic Mobile Ad-Hoc Network On-demand (DYMO) merupakan protokol *routing* reaktif yang menentukan jalur pada sumber yang ingin mengirim data ke tujuan. Protokol DYMO adalah penerus protokol AODV atau AODV*v2* dengan fitur *path accumulation*. Protokol DYMO menggunakan konsep *hop by hop routing* dari *sequence number* dan *link reversal*. Setiap *node* menyimpan *sequence number* masing-masing. *Sequence number* bertambah setiap kali *node* mengirimkan pesan permintaan rute. Hal ini memungkinkan *node* lain untuk menentukan urutan pesan penemuan untuk menghindari informasi *routing* menjadi basi, untuk mendeteksi pesan duplikat, dan untuk memastikan *loop* tanpa batas. Protokol ini memiliki dua operasi dasar: *Route discovery* and *Route maintenance*. (Deka & Khaturia, 2014).

Berikut merupakan proses *route discovery* dan *route maintenance* pada protokol DYMO (Kaur, 2014):

1. DYMO *Route Discovery*

   Proses *route discovery* pada protokol DYMO mirip dengan *route discovery* pada protokol AODV, tetapi pada protokol DYMO memiliki satu fitur tambahan yaitu *path accumulation*. *Node* 1 merupakan *node* sumber ingin berkomunikasi dengan *node* 6 yang merupakan tujuan. Awalnya dilakukan pengecekan rute ke *node* tujuan pada tabel *routing* jika tidak ada rute, maka akan *node* sumber akan mengirim pesan RREQ pada *node* tetangga terdekat. Ketika pesan RREQ dikirim, setiap *node* akan mensisipkan alamat *node* mereka sendiri pada pesan RREQ untuk

mekanisme jalur mundur (backward path). Pada akhirnya ketika *node* 6 (tujuan) menerima pesan RREQ, dan membuat pesan RREP yang akan dikiriman melalui mekanisme jalur mundur (backward path) dan proses *path accumulation* akan berjalan.



Gambar 2.5 DYMO *Route Discovery*

Sumber : (Kaur, 2014)

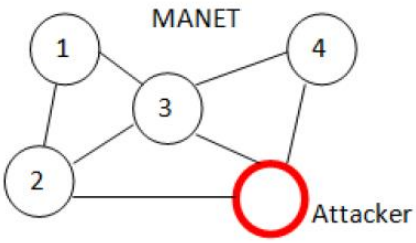
Proses ini memastikan bahwa jalur ke *node* tujuan dibuat dan setiap *node* mengetahui jalur ke *node* lainnya sepanjang rute.

2. DYMO *Route Maintenance*

Pada proses *route maintenance*, pesan RERR dibuat oleh *node* ketika jalur terputus pada rute yang telah ada dan pesan RERR akan dikirim ke *node-node* secara *multicast* yang bersangkutan pada jalur tersebut. Setiap *node* melakukan pembaharuan pada tabel *routing* masing-masing setelah menerima pesan RRER dan menghapus jalur yang rusak tersebut. *Node* sumber berhenti mengirim data melalui jalur yang rusak dan memulai kembali proses *route discovery* jika diperlukan.

2.4 Serangan *Black Hole*

Serangan *black hole* atau lubang hitam adalah salah satu ancaman keamanan dimana lalu lintas diarahkan ke *node* berbahaya yang sebenarnya tidak ada dalam jaringan. *black hole* merupakan analogi dunia nyata dengan lubang hitam di alam semesta dimana benda-benda menghilang (Puray & Palod, 2016). Pada serangan *black hole*, *node* penyerang akan berperilaku sebagai *node* normal pada jaringan. Setelah melakukan pengiriman data, *node* penyerang akan berperilaku sebagai *node* jahat sehingga paket data yang melewati *node* penyerang akan hilang (Khetmal, 2013).

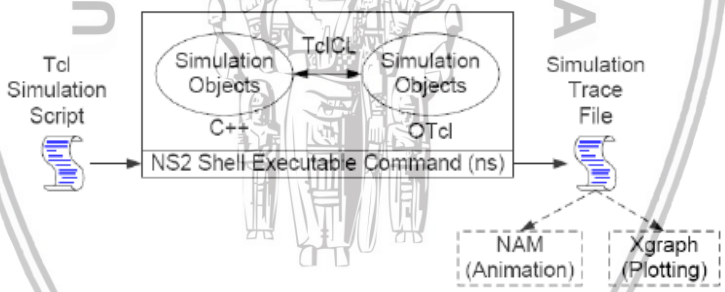


Gambar 2.6 Serangan *Black Hole*

Sumber : (Khetmal, 2013)

2.5 *Network simulator-2* (*NS-2*)

Network simulator (NS) merupakan simulator diskrit yang digunakan untuk melakukan penelitian pada sebuah jaringan. *NS* menyediakan dukungan untuk simulasi protokol *TCP*, *routing*, *multicast* melalui jaringan kabel dan nirkabel (lokal dan satelit). Terdapta 2 bahasa pemograman pada *NS-2*, pada *library* menggunakan bahasa pemograman C++ yang digunakan untuk *event scheduler, protocol* dan *network components*, dan bahasa pemograman *Tcl/OTcl* yang digunakan untuk menulis skrip simulasi. Gambar menunjukan hubungan antara *input* simulasi, proses eksekusi, dan *output* simulasi dengan kedua bahasa pemograman tersebut (Wirawan, 2004).



Gambar 2.7 *Network simulator-2*

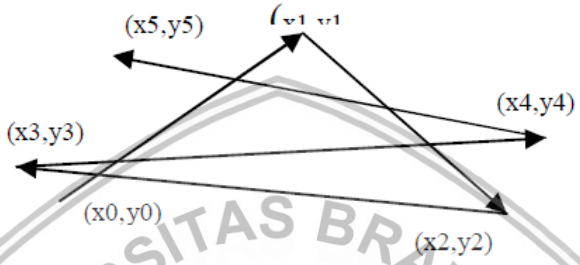
Sumber : (Wirawan, 2004)

Berikut merupakan komponen-komponen yang terdapat pada *NS-2* (Wirawan, 2004) :

1. NS sebagai simulator
2. NAM sebagai network animator yang bertugas dalam menampilkan *output* pada *NS-2*. Tampilan Nam berupa interface GUI yang dipanggil sebagai file berekstensi [.nam] pada skrip Tcl.
3. Preprocessing bertugas dalam membangun trafik dan topologi jaringan.
4. Postprocessing merupakan hasil simulasi yang ditampilkan pada file [.tr]. Hasil simulasi dapat dipilah menggunakan perintah awk dan dapat dikonversikan dalam bentuk grafik menggunakan XGraph.

2.6 Mobilitas *Random Way Point*

Mobilitas *Random Way Point* merupakan model pergerakan pengguna selular secara acak. Penentuan lokasi, kecepatan dapat berubah dari waktu ke waktu. *Node* selular akan memulai pergerakan setelah menunggu *pause time* yang telah ditentukan. Pergerakan akan memilih lokasi tujuan secara acak dalam cakupan area dan kecepatan acak didistribusikan merata antara *[min-speed, max-speed]*. Setelah mencapai lokasi tujuan, *node* selular menunggu lagi *pause time* sebelum memilih lokasi tujuan dan kecepatan yang baru (Sukhija, 2015).



Gambar 2.8 Mobilitas *Random Way Point*

Sumber : (Kute, 2014)

2.7 *Packet Delivery Ratio* (PDR)

Packet Delivery Ratio (PDR) merupakan perbandingan antara banyaknya paket yang diterima pada *node* tujuan dengan banyaknya paket yang dikirim oleh *node* tujuan. PDR dapat dihitung menggunakan persamaan sebagai berikut (Rohal, et al., 2013) :

$$\text{PDR} = \frac{prcv}{ptr}\ x\ 100\% \quad (2.1)$$

dengan:

prcv : jumlah paket data yang diterima oleh tujuan

ptr : jumlah paket data yang dikirim oleh sumber

PDR : *packet delivery ratio* (%)

2.8 *Normalized Routing Load* (NRL)

Normalized Routing Load (NRL) merupakan total paket *routing* yang dikirim dibagi dengan total paket data yang diterima. NRL dapat dihitung menggunakan persamaan sebagai berikut (Al-Maashri & Ould-Khaoua, 2006) :

$$\text{NRL} = \frac{pr}{prcv} \quad (2.2)$$

dengan:

pr : jumlah paket *routing*

prcv : jumlah paket data yang diterima oleh tujuan

NRL : *Normalized Routing Load*

2.9 *Packet Loss*

Packet Loss merupakan banyak paket yang hilang selama proses pengiriman data dari sumber ke tujuan. PL dapat dihitung menggunakan persamaan sebagai berikut (Rohal, et al., 2013) :

$$PL = \frac{ploss}{pt} \; x \; 100\% \tag{2.3}$$

dengan:

ploss : jumlah paket data yang hilang selama proses pengiriman data dari sumber ke tujuan

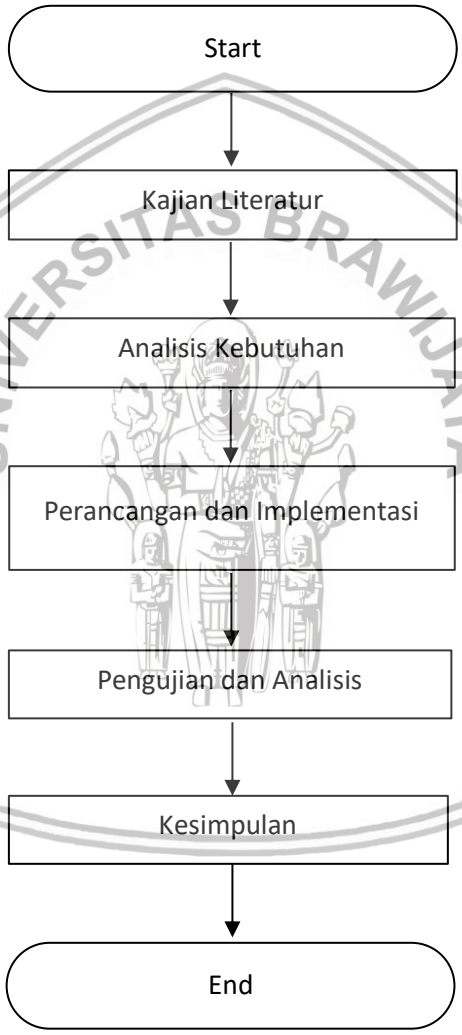
ptr : jumlah paket data yang dikirim oleh sumber

PL : *packet loss*

BAB 3 METODOLOGI

Pada bab ini menjelaskan langkah-langkah yang dilakukan dalam penelitian analisis dampak serangan *black hole* terhadap kinerja protokol AODV dan DYMO pada MANET (*Mobile Ad-Hoc Network*). Dimulai dari kajian literatur, analisis kebutuhan, perancangan dan implementasi, pengujian dan analisis, serta kesimpulan dan saran.

Berikut merupakan diagram alir urutan pengerjaan penelitian ini :



Gambar 3.1 Diagram Alir Penelitian

3.1 Kajian Literatur

Kajian literatur merupakan dasar teori yang digunakan dalam menunjang penulisan laporan. Pengetahuan tentang *mobile ad hoc network* (MANET) sebagai teori yang menunjang penulisan laporan.

3.2 Analisis Kebutuhan

Analisis kebutuhan diperlukan untuk mengidentifikasi dan menganalisis kebutuhan sistem yang digunakan untuk menunjang sistem bekerja sesuai tujuan. Analisis kebutuhuan dibagi menjadi dua yaitu kebutuhan fungsional dan kebutuhan non fungsional.

3.2.1 Kebutuhan Fungsional

Kebutuhan fungsional dilakukan untuk memberikan gambaran mengenai proses-proses yang dapat dilakukan oleh sistem, meliputi:

1. Sistem dapat mengimplementasikan protokol AODV dan protokol DYMO pada jaringan MANET dengan menggunakan simulator *NS-2*.
2. Sistem dapat mengimplementasikan serangan *black hole* terhadap protokol AODV dan protokol DYMO pada MANET.

3.2.2 Kebutuhan Non Fungsional

Kebutuhan non fungsional dilakukan untuk mengetahui spesifikasi kebutuhan untuk sistem, meliputi kebutuhan perangkat lunak dan kebutuhan perangkat keras yang digunakan dalam melakukan penelitian.

3.2.2.1 Kebutuhan Perangkat Keras

Kebutuhan perangkat keras dijelaskan segala kebutuhan perangkat keras (hardware) yang digunakan untuk sistem. Perangkat keras yang digunakan pada penelitian ini yaitu sebuah laptop untuk melakukan simulasi protokol *routing.* Berikut merupakan spesifikasi perangkat yang digunakan :

Prosesor	: Intel(R) Core(TM) i5-8250U
RAM	: 8 GB

3.2.2.2 Kebutuhan Perangkat Lunak

Kebutuhan perangkat lunak dijelaskan segala kebutuhan perangkat lunak (software) yang digunakan pada sistem. Perangkat lunak mencakup sistem operasi pada sistem dan aplikasi yang digunakan dalam melakukan penelitian. Berikut merupakan kebutuhan perangkat lunak untuk menunjang penelitian :

- Sistem operasi Ubuntu 16.04
- *Network simulator-2* (*NS-2*)
- Sublime Text

3.3 Perancangan dan Implementasi

Tahap perancangan dan implementasi memuat perancangan suatu sistem yang dapat memenuhi kebutuhan berdasarkan analisis kebutuhan yang dilakukan dan memuat implementasi protokol AODV dan protokol DYMO serta serangan

black hole pada MANET menggunakan simulator *NS-2*. Tahap Implementasi dibuat sesuai dengan spesifikasi sistem yang telah dirancang pada tahap perancangan.

3.4 Pengujian dan Analisis

Tahap pengujian dan analisis, dijelaskan pengujian yang dilakukan dengan beberapa skenario simulasi yaitu kepadatan 40 *node* dengan variasi jumlah *node* penyerang *(black hole,* kepadatan 60 *node* dengan variasi jumlah *node* penyerang (*black hole*)*,* dan kepadatan 80 *node* dengan variasi jumlah *node* penyerang (*black hole*)*.* Pengujian dilakukan guna menganalisis dampak serangan *black hole* terhadap kinerja protokol AODV dan protokol DYMO menggunakan simulator *NS-2* dan melakukan analisis dampak serangan *black hole* terhadap kinerja protokol AODV dan protokol DYMO yang telah dilakukan pada tahap pengujian dengan menggunakan parameter *packet delivery ratio*, *normalized routing load* dan *packet loss*.

3.5 Kesimpulan

Tahap kesimpulan dilakukan setelah tahap pengujian dan analisis. Kesimpulan diambil dengan menganalisis hasil dari penelitian yang telah dilakukan, guna untuk memberikan rekomendasi penelitian selanjutnya.

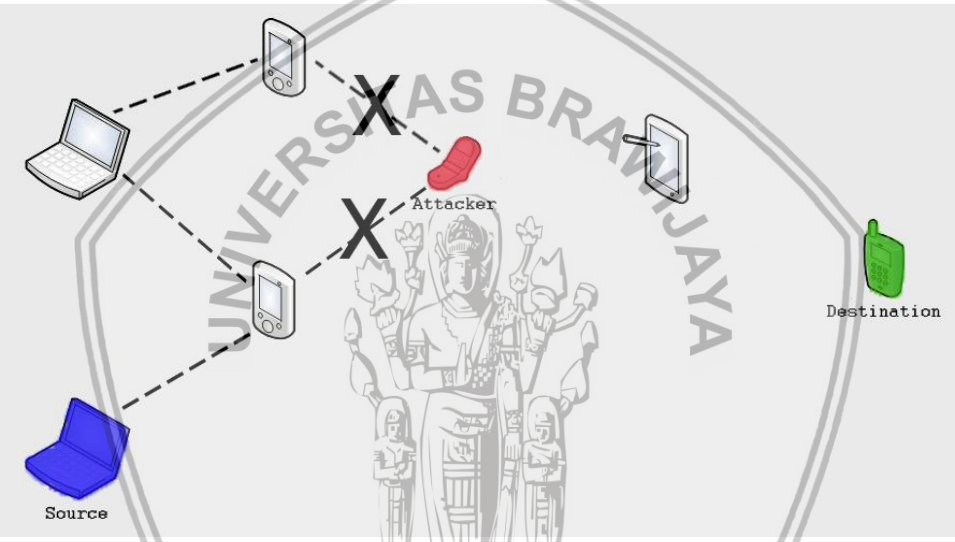
BAB 4 PERANCANGAN DAN IMPLEMENTASI

4.1 Perancangan

Tahap ini akan dilakukan perancanan yang dibutuhkan dalam melakukan implementasi protokol AODV dan protokol DYMO serta serangan *black hole* pada simulasi jaringan MANET meliputi topologi jaringan, skenario simulasi, parameter kinerja, dan serangan *black hole.*

4.1.1 Topologi Jaringan

Topologi jaringan menjelaskan mengenai rancangan topologi yang digunakan dalam implementasi protokol *routing*. Berikut merupakan topologi jaringan protokol *routing* MANET:



Gambar 4.1 Topologi Jaringan MANET dengan Serangan *Black Hole*

Gambar 4.1 merupakan perancangan topologi jaringan yang akan diimplementasikan pada pengujian bervariasi *node* serangan (*black hole*). Pengujian yang dilakukan menggunakan kepadatan *node* sebanyak 40, 60, dan 80 dengan variasi *node* serangan sebanyak 5, 10, 15, dan 20 *node*. Laptop dan *handphone* menggambarkan *node-node* pada MANET yang akan bergerak secara acak menggunakan pergerakan *Random Way Point*. *Node* sumber ditetapkan berwarna biru, *node* tujuan ditetapkan berwarna hijau, dan *node attacker* (*black hole*) ditetapkan berwarna merah untuk lebih mudah mengetahui letak posisi *node* sumber, *node* tujuan, dan *node attacker* (*black hole*) ketika *node-node* bergerak.

4.1.2 Skenario Simulasi

Skenario simulasi merupakan parameter-parameter yang akan digunakan dalam melakukan simulasi. Parameter secara lengkap yang digunakan untuk merancang skenario ditunjukan pada tabel 4.1.

Tabel 4.1 Parameter Simulasi

Parameter	Atribut
Kepadatan Jumlah *Node*	40, 60, dan 80
Protokol *Routing*	AODV dan DYMO
Sumber Trafik	UDP
Ukuran Paket	512 byte
Luas Area	1000x1000 m^2
Tipe Serangan	*Black Hole*
Variasi *Node* Penyerangan (*black hole*)	5, 10, 15, 20
Model Pergerakan	Random Way Point
Kecepatan *Node*	2 m/s
Waktu simulasi	1000 s
Simulator	*Network simulator-2*

Tabel 4.1 menjelaskan parameter simulasi yang akan digunakan pada tahap implementasi simulasi. Protokol yang digunakan yaitu protokol AODV dan protokol DYMO. Kepadatan *node* yang digunakan sebanyak 40, 60, dan 80. Penggunaan kepadatan *node* tersebut berkaitan dengan luas area yang digunakan yaitu 1000x1000 m^2 sehingga pada luas area tersebut, kepadatan 40 *node* digambarkan sebagai kepadatan yang sepi, kepadatan 60 *node* digambarkan sebagai kepadatan yang sedang, dan kepadatan 80 *node* digambarkan sebagai kepadatan yang ramai. Sumber trafik menggunakan UDP dengan ukuran paket 512 *byte*. Tipe serangan yang digunakan yaitu serangan *black hole* yang bersifat internal dengan variasi *node* penyerang (*black hole*) sebanyak 5, 10, 15, dan 20. Variasi *node* penyerang (*black hole*) menggunakan jumlah *black hole* yang besar sehingga dapat melihat kondisi terburuk pada kedua protokol. Model pergerakan menggunakan *random way point* dengan kecepatan 2 m/s dan menggunakan *network simulator-2* untuk mensimulasikan kedua protokol.

4.1.3 Parameter Kinerja

Protokol *routing* AODV dalam melakukan pembaruan tabel *routing* hanya mengetahui *node* sumber dan tujuan, sedangkan protokol *routing* DYMO memiliki kemampuan untuk mengetahui informasi tentang semua *node* antara *node* sumber dan tujuan di jalur yang baru.

Selain perbedaan tersebut, penulis ingin mengetahui bagaimana perbedaan unjuk kerja protokol *routing* AODV dan DYMO berdasarkan parameter *packet delivery ratio*, *normalized routing load,* dan *packet loss*.

1. *Packet Delivery Ratio*

   Packet Delivery Ratio (PDR) adalah rasio antara banyaknya paket yang diterima oleh tujuan dengan banyaknya paket yang dikirim oleh sumber. PDR dapat menjadi acuan untuk membandingkan kedua protokol ketika terjadi serangan *black hole* serta dalam jumlah kepadatan *node* karena *node* sumber akan mengirimkan paket ke *node* tujuan secara berkala.

   $$\text{PDR} = \frac{prcv}{ptr}\ x\ 100\%$$

   dengan:

   prcv : jumlah paket data yang diterima oleh tujuan

   ptr : jumlah paket data yang dikirim oleh sumber

   PDR : *packet delivery ratio* (%)

2. *Normalized Routing Load*

   Normalized Routing Load (NRL) adalah ratio antara jumlah paket *routing* dengan paket data yang diterima oleh tujuan. *Normalized Routing Load* dapat menjadi parameter untuk membandingkan kedua protokol karena setiap protokol akan melakukan paket *routing* yang berbeda untuk menemukan jalur dari *node* sumber ke *node* tujuan.

   $$\text{NRL} = \frac{pr}{prcv}$$

   dengan:

   pr : jumlah paket *routing*

   prcv : jumlah paket data yang diterima oleh tujuan

   NRL : *normalized routing load*

3. *Packet Loss*

   Packet Loss adalah banyak paket yang hilang selama proses pengiriman data dari sumber ke tujuan. *Packet Loss* digunakan untuk membandingkan kedua protokol pada saat terdapat paket hilang yang disebabkan oleh serangan *black hole.*

   $$PL = \frac{plBhole}{ptr}\ x\ 100\%$$

   dengan:

   plBhole : jumlah paket data yang hilang selama proses pengiriman data dari sumber ke tujuan yang disebabkan oleh serangan *black hole*

   ptr : jumlah paket data yang dikirim oleh sumber

   PL : *packet loss*

4.1.4 Serangan *Black Hole*

Pada simulasi ini, *node* penyerang akan berperilaku seperti layaknya *node* biasa, yaitu akan melakukan broadcast untuk pembentukkan jalur *routing*. Apabila ada paket data yang diteruskan melalui *node* penyerang, maka paket tersebut akan di *drop* dan tidak akan sampai pada tujuan. *Node* penyerang yang dilakukan bersifat statis pada setiap variasi kepadatan *node* dan terdapat variasi jumlah *node* penyerang pada setiap pengujian serangan *black hole.*

4.2 Implementasi

Tahap ini akan dilakukan implementasi simulasi protokol *routing* AODV dan DYMO pada MANET dengan menggunakan simulator *NS-2*. Implementasi dilakukan sesuai dengan spesifikasi sistem yang telah dirancang pada tahap perancangan.

4.2.1 Konfigurasi *Network simulator-2*

Penelitian ini diimplementasikan menggunakan simulator *NS-2*. Dalam mengimplementasikan perancangan yang telah ditetapkan sebelumnya, dibutuhkan beberapa konfigurasi dalam menerapkan perancangan tersebut pada *NS-2*. Konfigurasi tersebut diatur dalam *file script* Tcl, sehingga dibutuhkan dua file *script* Tcl yang mewakili masing-masing protokol *routing* yaitu AODV.tcl dan DYMO.tcl.

4.2.1.1 Konfigurasi Parameter Simulasi

Konfigurasi parameter simulasi dilakukan sebagai implementasi dari rancangan parameter yang telah dibuat pada tahap perancangan dan diterapkan pada *NS-2*. Konfigurasi parameter simulasi diatur pada *file script* Tcl yang telah dibuat, yaitu AODV.tcl dan DYMO.tcl dengan konfigurasi sebagai berikut:

Tabel 4.2 Konfigurasi Parameter Simulasi

```
1   set opt(chan)       Channel/WirelessChannel                 ;
2   set opt(prop)       Propagation/TwoRayGround                ;
3   set opt(netif)      Phy/WirelessPhy                         ;
4   set opt(mac)        Mac/802_11                              ;
5   set opt(ifq)        Queue/DropTail/PriQueue                 ;
6   set opt(ll)         LL                                      ;
7   set opt(ant)        Antenna/OmniAntenna                     ;
8   set opt(ifqlen)     50                                      ;
9   set opt(nn)         40/60/80                                ;
10  set opt(minSpeed)   0.5                                     ;
11  set opt(maxSpeed)   2                                       ;
12  set opt(rp)         AODV/DYMOUM                             ;
13  set opt(seed)       1                                       ;
14  set opt(x)          1000                                    ;
15  set opt(y)          1000                                    ;
16  set opt(stop)       1000                                    ;
```

Penjelasan:

1. Baris 1-8 mendefinisikan tipe *channel*, model propagasi yang digunakan, tipe jaringan *interface*, tipe *mac*, tipe *queue interface*, tipe *link layer*, model

antenna yang digunakan, dan jumlah ukuran paket *node* yang digunakan.

2. Baris 9 mendefinisikan jumlah *mobile node* yang akan digunakan yakni 40, 60, dan 80.
3. Baris 10-11 mendefinisikan kecepatan minimal dan maksimal selama simulasi dalam satuan *m/s*.
4. Baris 12 mendefinisikan protokol *routing* yang akan digunakan yakni AODV untuk protokol AODV dan DYMO*UM* untuk protokol DYMO.
5. Baris 13 mendefinisikan seed yang digunakan untuk penentuan lokasi setiap *node* pada fungsi *pseudo-random*.
6. Baris 14-15 mendefinisikan luas area jaringan sumbu X dan sumbu Y.
7. Baris 16 mendefinisikan waktu simulasi yang digunakan yakni 1000 detik.

4.2.1.2 Konfigurasi Topologi Jaringan

Konfigurasi topologi jaringan dilakukan sebagai implementasi dari rancangan topologi yang telah dibuat. Setiap skenario memiliki jumlah *node* yang berbeda yaitu 40, 60, dan 80. Perancangan dilakukan menyesuaikan karakteristik dari MANET, dimana *Node-node* bergerak bebas secara acak dengan arah dan posisi yang tidak tentu. Namun, pada perancangan ini *node* sumber dan tujuan dibuat saling berjauhan pada detik ke-0. Konfigurasi topologi jaringan diatur pada *file script* Tcl yang telah dibuat, yaitu AODV.tcl dan DYMO.tcl dengan konfigurasi sebagai berikut:

Tabel 4.3 Konfigurasi Topologi Jaringan

```
1  set genSeed [new RNG]
2  $genSeed seed $opt(seed)
3  set randomSeed [new RandomVariable/Uniform]
4  $randomSeed use-rng $genSeed
5  $randomSeed set min_ 1.0
6  $randomSeed set max_ 1000.0
7
8  set genNodeX [new RNG]
9  $genNodeX seed [expr [$randomSeed value]]
10 set randomNodeX [new RandomVariable/Uniform]
11 $randomNodeX use-rng $genNodeX
12 $randomNodeX set min_ 1.0
13 $randomNodeX set max_ [expr $opt(x) - 1.0]
14
15 set posNodeY [new RNG]
16 $posNodeY seed [expr [$randomSeed value]]
17 set randomNodeY [new RandomVariable/Uniform]
18 $randomNodeY use-rng $posNodeY
19 $randomNodeY set min_ 1.0
20 $randomNodeY set max_ [expr $opt(y) - 1.0]
21
22 set genNodeSpeed [new RNG]
23 $genNodeSpeed seed [expr [$randomSeed value]]
24 set randomNodeSpeed [new RandomVariable/Uniform]
25 $randomNodeSpeed use-rng $genNodeSpeed
26 $randomNodeSpeed set min_ $opt(minSpeed)
27 $randomNodeSpeed set max_ $opt(maxSpeed)
28
29 for {set i 0} {$i < $opt(nn)} {incr i} {
```

```
30      set node_($i) [$ns_ node]
31  }
32
33  for {set i 0} {$i < $opt(nn)} {incr i} {
34        set X [expr [$randomNodeX value] ]
35        $node_($i) set X_ $X
36        set Y [expr [$randomNodeY value] ]
37        $node_($i) set Y_ $Y
38        $node_($i) set Z_ 0.0
39        $node_(0) set X_ 1
40        $node_(0) set Y_ 1
41        $node_(0) set Z_ 0.0
42        $node_(1) set X_ 999
43        $node_(1) set Y_ 999
44        $node_(1) set Z_ 0.0
45  }
```

Penjelasan:

1. Baris 1-6 merupakan fungsi pseudo-random sequence generator untuk menghasilnya urutan angka secara tidak teratur yang digunakan dalam menentukan penempatan setiap *node* secara random.
2. Baris 8-13 merupakan fungsi *pseudo-random* untuk menetapkan letak koordinat X yang akan digunakan untuk penempatan koordinat X setiap *node* secara random.
3. Baris 15-20 merupakan fungsi *pseudo-random* untuk menetapkan letak koordinat Y yang akan digunakan untuk penempatan koordinat Y setiap *node* secara random.
4. Baris 22-27 merupakan fungsi *pseudo-random* untuk menetapkan kecepatan yang akan digunakan untuk kecepatan pada setiap *node* secara random.
5. Baris 29-31 merupakan fungsi perulangan untuk melakukan perulangan sesuai dengan banyak jumlah *node* yang di konfigurasikan dan *node-node* tersebut akan dimasukan pada *node*_($i) [$ns_ *node*].
6. Baris 33-38 mendefinisikan letak koordinat X dan Y pada setiap *node* menggunakan nilai yang dihasilkan pada fungsi *pseudo-random* $random*Node*X value dan $random*Node*Y value.
7. Baris 39-44 mendefinisikan letak koordinat X dan Y pada sumber dan tujuan yang saling berjauhan.

4.2.1.3 Konfigurasi Pergerakan *Node*

Konfigurasi pergerakan *node* dilakukan sebagai implementasi dari perancangan skenario simulasi pergerakan tiap *node*. Model pergerakan yang digunakan pada penelitian ini yaitu model pergerakan *Random Way Point*. Konfigurasi pergerakan *node* diatur pada *file script* Tcl yang telah dibuat, yaitu AODV.tcl dan DYMO.tcl dengan konfigurasi sebagai berikut:

Tabel 4.4 Konfigurasi Pergerakan *Node*

```
1   for {set i 0} {$i < $opt(nn)} {incr i} {
2         set xr_ [$randomNodeX value]
3         set yr_ [$randomNodeY value]
4         set spd_ [$randomNodeSpeed value]
```

```
5       $ns_ at 0 "$node_($i) setdest $xr_ $yr_ $spd_";
6       set xr1_ [$randomNodeX value]
7       set yr1_ [$randomNodeY value]
8       set spd1_ [$randomNodeSpeed value]
9       $ns_ at 400 "$node_($i) setdest $xr1_ $yr1_ $spd1_";
10  }
```

Penjelasan:

1. Baris 1 merupakan fungsi perulangan untuk melakukan perulangan sesuai dengan banyak jumlah *node* yang di konfigurasikan.
2. Baris 2-4 medefinisikan arah koordinat X, Y dan kecepatan menggunakan masukan nilai dari fungsi *pseudo-random* dan dimasukan pada variable xr, yr, dan spd.
3. Baris 5 melakukan pergerakan pada setiap *node* dari detik ke-0 menggunakan arah koordinat xr, yr, dan spd yang telah didefinisikan.
4. Baris 6-8 medefinisikan arah koordinat X, Y dan kecepatan menggunakan masukan nilai dari fungsi *pseudo-random* dan dimasukan pada variable xr1, yr1, dan spd1.
5. Baris 9 melakukan pergerakan pada setiap *node* dari detik ke-400 menggunakan arah koordinat xr1, yr1, dan spd1 yang telah didefinisikan.

4.2.1.4 Konfigurasi Aliran Trafik Data

Konfigurasi aliran trafik data dilakukan sebagai implementasi dari perancangan pengiriman paket data dari *node* sumber ke *node* tujuan. Aliran trafik data yang digunakan pada penelitian ini yaitu aliran trafik data UDP dan model pengiriman CBR. Konfigurasi aliran trafik data diatur pada *file script* Tcl yang telah dibuat, yaitu AODV.tcl dan DYMO.tcl dengan konfigurasi sebagai berikut:

Tabel 4.5 Konfigurasi Aliran Trafik Data

```
1   set udp_(0) [new Agent/UDP]
2   $ns_ attach-agent $node_(0) $udp_(0)
3   set null_(0) [new Agent/Null]
4   $ns_ attach-agent $node_(1) $null_(0)
5   set cbr_(0) [new Application/Traffic/CBR]
6   $cbr_(0) set packetSize_ 512
7   $cbr_(0) set interval_ 1
8   $cbr_(0) attach-agent $udp_(0)
9   $ns_ connect $udp_(0) $null_(0)
10  $ns_ at 0.0 "$cbr_(0) start"
```

Penjelasan:

1. Baris 1 melakukan pembentukan koneksi melalui protokol *UDP*.
2. Baris 2 menetapkan *node* 0 sebagai *node* sumber.
3. Baris 3-4 menetapkan *node* 1 sebagai *node* tujuan.
4. Baris 5 melakukan pembentukan trafik *CBR* pada protokol *UDP*.
5. Baris 6 mendefinisikan ukuran paket yang akan dikirim yakni 512 *byte*.
6. Baris 7 mendefinisikan interval pengiriman data yang digunakan yaitu 1 detik.
7. Baris 8 menetapkan aplikasi *CBR* pada protokol *UDP*.

8. Baris 9 merupakan pembuatan koneksi antara *node* sumber dan *node* tujuan.
9. Baris 10 memulai koneksi *CBR* pada detik ke-0.

4.2.1.5 Konfigurasi Pemrosesan Data *Output*

Konfigurasi pemrosesan data *output* dilakukan sebagai pengaturan akhir skenario simulasi sehingga data *output* dapat diproses sesusai pengujian yang ingin dilakukan. Konfigurasi pemrosesan data *output* diatur pada *file script* Tcl yang telah dibuat, yaitu AODV.tcl dan DYMO.tcl dengan konfigurasi sebagai berikut:

Tabel 4.6 Konfigurasi Pemrosesan Data *Output*

```
1  set tracefd  [open hasil.tr w]
2  $ns_ trace-all $tracefd
3  set namtrace [open hasil.nam w]
4  $ns_ namtrace-all-wireless $namtrace $opt(x) $opt(y)
```

Penjelasan:

1. Baris 1-2 mendefinisikan nama *tracefile* dan menampilkan *tracefile.*
2. Baris 3-4 mendefinisikan nama *namfile* dan menampilakn *nam tracefile*.

4.2.1.6 Konfigurasi Serangan *Black Hole*

Konfigurasi serangan *black hole* dilakukan sebagai implementasi dari perancangan skenario variasi serangan *black hole* yaitu 0, 5, 10, 15, dan 20. Konfigurasi dilakukan dengan menambahkan *source code black hole* didalam *file* AODV.h dan AODV.cc pada protokol *routing* AODV dan untuk protokol *routing* DYMO menambahkan *source code black hole* didalam *file* DYMO_um.h dan DYMO_um.cc dengan konfigurasi sebagai berikut:

1. Protokol AODV

Tabel 4.7 Konfigurasi Serangan *Black Hole* pada file AODV.h

```
.   .
.   .
271         /*
272         * History management
273         */
274
275        double      PerHopTime(AODV_rt_entry *rt);
276        bool        malicious;
277        nsaddr_t        index;     // IP Address of this node
278        u_int32_t       seqno;     // Sequence Number
279        int             bid;       // Broadcast ID
.   .
.   .
```

Penjelasan:

1. Baris 276 melakukan inisiasi bool malicious pada *file* AODV.h agar variable *malicious* dapat digunakan pada *file* AODV.cc.

Setelah melakukan inisiasi variable *malicious* pada *file* AODV.h dilanjutkan dengan melakukan konfigurasi serangan *black hole* pada *file* AODV.cc. Berikut merupakan konfigurasi serangan *black hole* pada *file* AODV.cc :

Tabel 4.8 Konfigurasi Serangan *Black Hole* pada file AODV.cc

```
.   .
.   .
75  int
76  AODV::command(int argc, const char*const* argv) {
77    if(argc == 2) {
78    Tcl& tcl = Tcl::instance();
79
80      if(strncasecmp(argv[1], "id", 2) == 0) {
81        tcl.resultf("%d", index);
82        return TCL_OK;
83      }
84      if(strncasecmp(argv[1], "Black Hole", 6) == 0) {
85       malicious = true;
86        return TCL_OK;
87      }
.   .
.   .
145 AODV::AODV(nsaddr_t id) : Agent(PT_AODV),
146       btimer(this), htimer(this), ntimer(this),
147       rtimer(this), lrtimer(this), rqueue() {
148
149   index = id;
150   seqno = 2;
151   bid = 1;
152   malicious = false;
.   .
.   .
445 void
446 AODV::rt_resolve(Packet *p) {
447 struct hdr_cmn *ch = HDR_CMN(p);
448 struct hdr_ip *ih = HDR_IP(p);
449 AODV_rt_entry *rt;
450       if (malicious == true ) {
451          drop(p, DROP_BHOLE);
452           return;
453        }
.   .
.   .
```

Penjelasan:

1. Baris 84-87 merupakan fungsi untuk membuat *black hole* dengan menetapkan *node* sebagai *Black Hole* pada konfigurasi dan akan merubah variable *malicious* menjadi *true*.
2. Baris 152 menginisiasi variable *malicious* = *false*.
3. Baris 450-453 merupakan fungsi untuk melakukan *drop* paket yang diterima jika *node* tersebut merupakan *node black hole.*

2. Protokol DYMO

Tabel 4.9 Konfigurasi Serangan *Black Hole* pada *file* DYMO_um.h

```
.   .
.   .
90      protected:
91      Mac                 *mac_;
92      Trace               *logtarget_;
93      DYMOUM_QueueTimer qtimer_;
94      nsaddr_t            ra_addr_;
95      int                 initialized_;
96      bool                malicious;.
.   .
.   .
```

Penjelasan:

1. Baris 96 melakukan inisiasi bool malicious pada *file* DYMO_um.h agar variable *malicious* dapat digunakan pada *file* DYMO_um.cc.

Setelah melakukan inisiasi variable *malicious* pada *file* DYMO_um.h dilanjutkan dengan melakukan konfigurasi serangan *black hole* pada *file* DYMO_um.cc. Berikut merupakan konfigurasi serangan *black hole* pada *file* DYMO_um.cc :

Tabel 4.10 Konfigurasi Serangan *Black Hole* pada file DYMO_um.cc

```
.   .
.   .
65  NS_CLASS    DYMOUM(nsaddr_t    id)    :    Agent(PT_DYMOUM),
    qtimer_(this),
66                          initialized_(0), pq_len(0)
67  {
68      malicious = false;
69      bind_bool("no_path_acc_", &no_path_acc);
70      bind_bool("reissue_RREQ_", &reissue_RREQ);
71      bind_bool("s_bit_", &s_bit);
72      bind("hello_ival_", &hello_ival);
.   .
.   .
128 int
129 NS_CLASS command(int argc, const char*const* argv) {
130     if (argc == 2) {
131         if (strcasecmp(argv[1], "Black Hole") == 0) {
132         malicious = true;
133             return TCL_OK;
134         }
135         if (strcasecmp(argv[1], "start") == 0) {
136             return start();
137         }
138     }
.   .
.   .
236 void
237 NS_CLASS process_data(Packet *p) {
238     struct hdr_cmn* ch      = HDR_CMN(p);
239     struct hdr_ip* ih = HDR_IP(p);
```

```
240         ch->direction() = hdr_cmn::DOWN;
241         ch->addr_type() = NS_AF_INET;
242         if ((u_int32_t) ih->daddr() == IP_BROADCAST)
243         ch->next_hop_ = IP_BROADCAST;
244         else {
245               struct in_addr dest_addr;
246               dest_addr.s_addr  = ih->daddr();
247               rtable_entry_t *entry   =
    rtable_find(dest_addr);
248               if (!entry || entry->rt_state == RT_INVALID) {
249                     if (ih->saddr() == ra_addr_) {
250                           packet_queue_add(p, dest_addr);
251                           route_discovery(dest_addr);
252                     }
253                     else {
254                           if (entry->rt_is_used)
255                                 RERR_send(dest_addr,
    NET_DIAMETER, entry);
256                           drop(p, DROP_RTR_NO_ROUTE);
257                     }
258                     schedule_next_event();
259                     return;
260               }
261               else
262               {
263                     ch->prev_hop_ = ra_addr_;
264                     ch->next_hop_ =
265                           (nsaddr_t)                    entry-
    >rt_nxthop_addr.s_addr;
266                     if (hello_ival <= 0)
267                     {
268                           ch->xmit_failure_ =
    DYMOum_mac_failed_callback;
269                           ch->xmit_failure_data_  =  (void  *)
    this;
270                     }
271                     rtable_update_timeout(entry);
272                     dlog(LOG_DEBUG, 0, __FUNCTION__,
273                           "route to dst %s updated",
274                           ip2str(ih->daddr()));
275               }
276               if (malicious == true ) {
277               drop(p, DROP_BHOLE);
278               return;
279         }
280         }
281         Scheduler::instance().schedule(target_, p, 0.0);
282         schedule_next_event();
283   }
.     .
.     .
```

Penjelasan:

1. Baris 68 menginisiasi variable *malicious* = *false*.
2. Baris 131-134 merupakan fungsi untuk membuat *black hole* dengan menetapkan *node* sebagai *Black Hole* pada konfigurasi dan akan merubah variable *malicious* menjadi *true*.

3. Baris 276-278 merupakan fungsi untuk melakukan *drop* paket yang diterima jika *node* tersebut merupakan *node black hole.*

Berikutnya pengaturan serangan *black hole* pada file tcl. Pengaturan dilakukan untuk menetapkan *node* tertentu menjadi *node black hole.* Berikut konfigurasi serangan *black hole* pada file tcl:

Tabel 4.11 Konfigurasi Serangan *Black Hole* pada file tcl

```
1  $ns_ at 0.0 "[$node_(2) set ragent_] blackhole"
2  $ns_ at 0.0 "[$node_(3) set ragent_] blackhole"
3  $ns_ at 0.0 "[$node_(4) set ragent_] blackhole"
4  $ns_ at 0.0 "[$node_(5) set ragent_] blackhole"
5  $ns_ at 0.0 "[$node_(6) set ragent_] blackhole"
6  $ns_ at 0.0 "[$node_(7) set ragent_] blackhole"
7  $ns_ at 0.0 "[$node_(8) set ragent_] blackhole"
8  $ns_ at 0.0 "[$node_(9) set ragent_] blackhole"
```

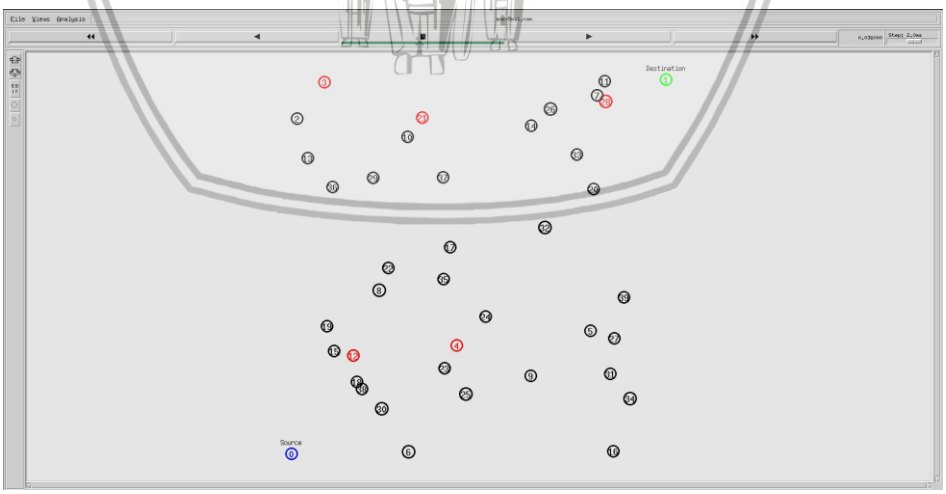
Penjelasan:

1. Baris 1-10 menetapkan *node-node* sebagai *node black hole* pada saat simulasi dimulai.

4.2.2 Topologi Jaringan dengan Serangan *Black Hole*

Topologi jaringan dengan serangan *black hole* dibuat berdasarkan parameter yang telah ditentukan. *Node* pada topologi jaringan sebanyak 40, 60, 80 dengan variasi *node* penyerang sebanyak 5, 10, 15, 20. Berikut merupakan topologi jaringan menggunakan serangan *black hole* pada kepadatan *node* sebanyak 40, 60, 80 dengan variasi *node* penyerang sebanyak 5, 10, 15, 20.

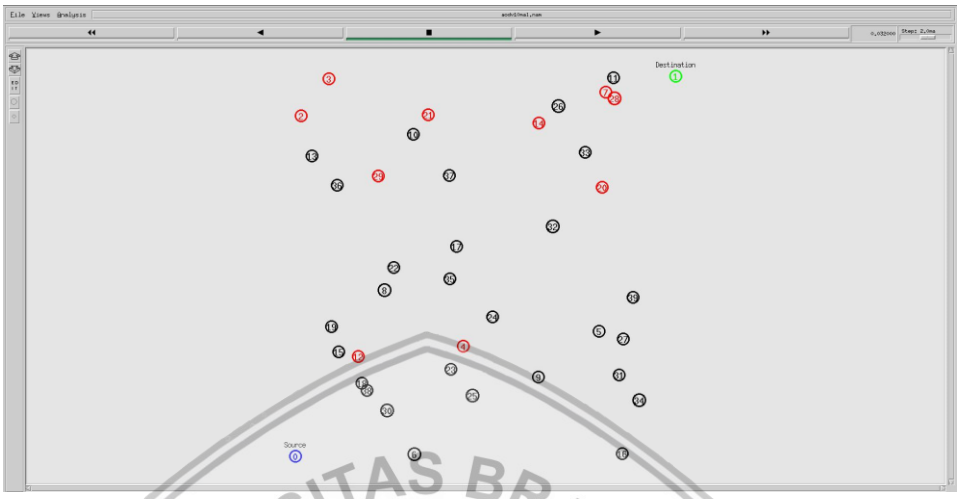
1. Topologi Jaringan 40 *node* dengan Serangan *Black Hole*



Gambar 4.2 Topologi Jaringan 40 *node* dengan variasi 5 *node Black Hole*

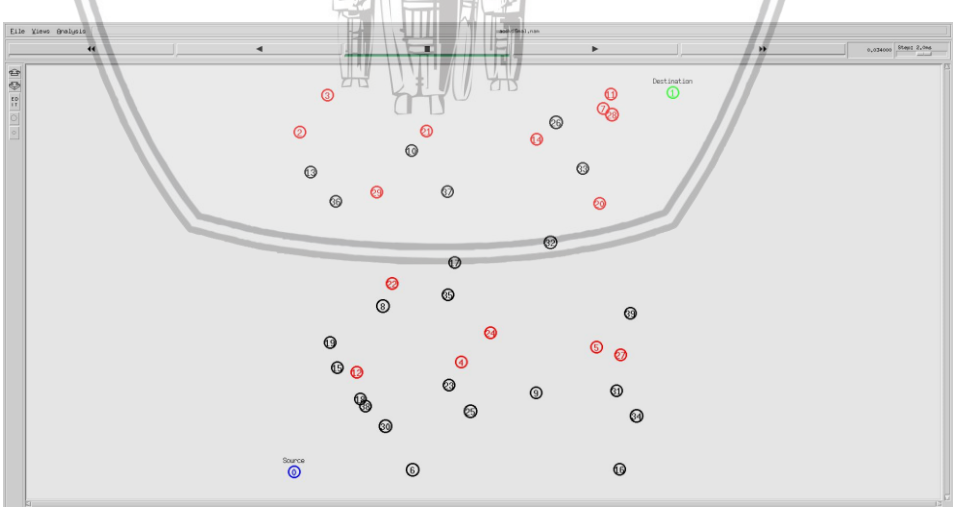
Gambar 4.6 merupakan simulasi dari topologi jaringan dengan jumlah *node* sebanyak 40 dengan variasi 5 *node black hole. Node* 0 yang berwarna biru ditetapkan sebagai *node* sumber dan *node* 1 yang berwarna hijau ditetapkan sebagai *node* tujuan. *Node-node* yang berwarna hitam merupakan *Node-node*

yang akan dilewatkan paket dari sumber ke tujuan. *Node* sumber dan *node* tujuan diletakkan saling berjauhan agar dapat memaksimalkan pengujian yang akan dilakukan.



Gambar 4.3 Topologi Jaringan 40 *node* dengan varaiasi 10 *node Black Hole*

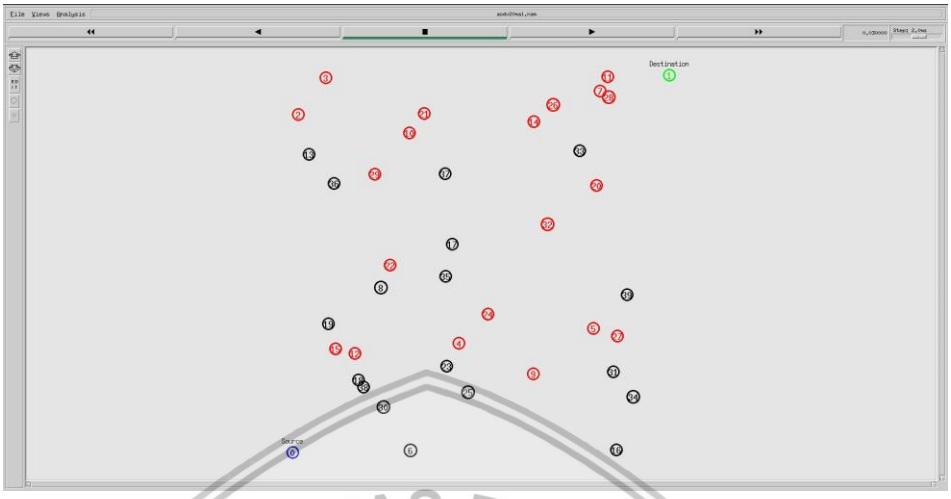
Gambar 4.7 merupakan simulasi dari topologi jaringan dengan jumlah *node* sebanyak 40 dengan variasi 10 *node black hole. Node* 0 yang berwarna biru ditetapkan sebagai *node* sumber dan *node* 1 yang berwarna hijau ditetapkan sebagai *node* tujuan. *Node-node* yang berwarna hitam merupakan *Node-node* yang akan dilewatkan paket dari sumber ke tujuan. *Node* sumber dan *node* tujuan diletakkan saling berjauhan agar dapat memaksimalkan pengujian yang akan dilakukan.



Gambar 4.4 Topologi Jaringan 40 *node* dengan variasi 15 *node Black Hole*

Gambar 4.8 merupakan simulasi dari topologi jaringan dengan jumlah *node* sebanyak 40 dengan variasi 15 *node black hole. Node* 0 yang berwarna biru ditetapkan sebagai *node* sumber dan *node* 1 yang berwarna hijau ditetapkan sebagai *node* tujuan. *Node-node* yang berwarna hitam merupakan *Node-node* yang akan dilewatkan paket dari sumber ke tujuan. *Node* sumber dan *node* tujuan

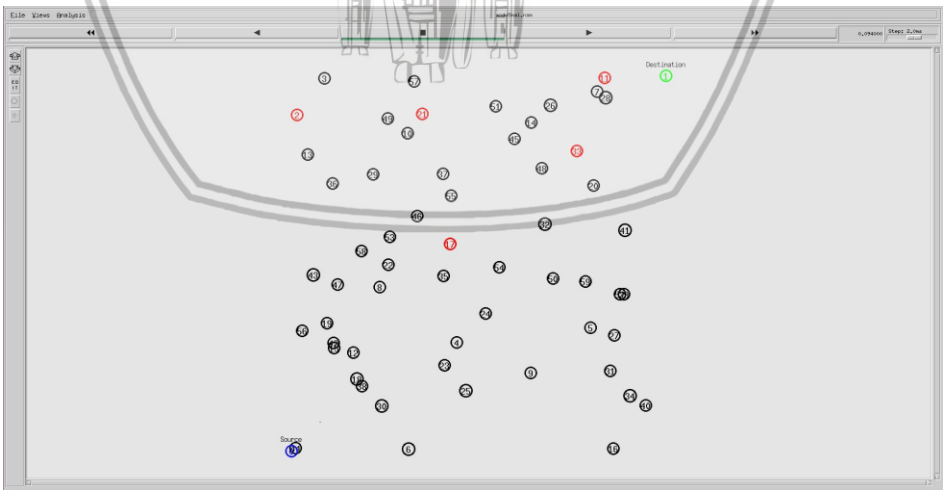
diletakkan saling berjauhan agar dapat memaksimalkan pengujian yang akan dilakukan.



Gambar 4.5 Topologi Jaringan 40 *node* dengan variasi 20 *node Black Hole*

Gambar 4.9 merupakan simulasi dari topologi jaringan dengan jumlah *node* sebanyak 40 dengan variasi 20 *node black hole. Node* 0 yang berwarna biru ditetapkan sebagai *node* sumber dan *node* 1 yang berwarna hijau ditetapkan sebagai *node* tujuan. *Node-node* yang berwarna hitam merupakan *Node-node* yang akan dilewatkan paket dari sumber ke tujuan. *Node* sumber dan *node* tujuan diletakkan saling berjauhan agar dapat memaksimalkan pengujian yang akan dilakukan.

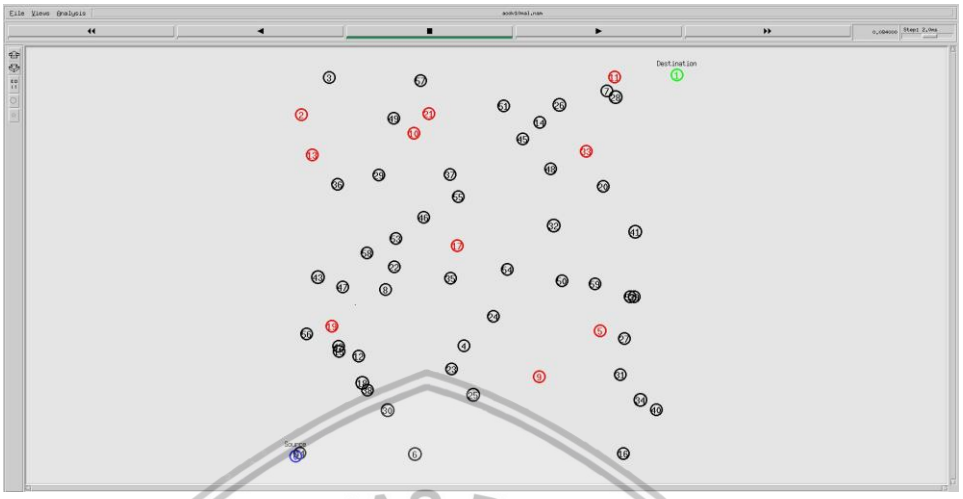
2. Topologi Jaringan 60 *node* dengan Serangan *Black Hole*



Gambar 4.6 Topologi Jaringan 60 *node* dengan variasi 5 *node Black Hole*

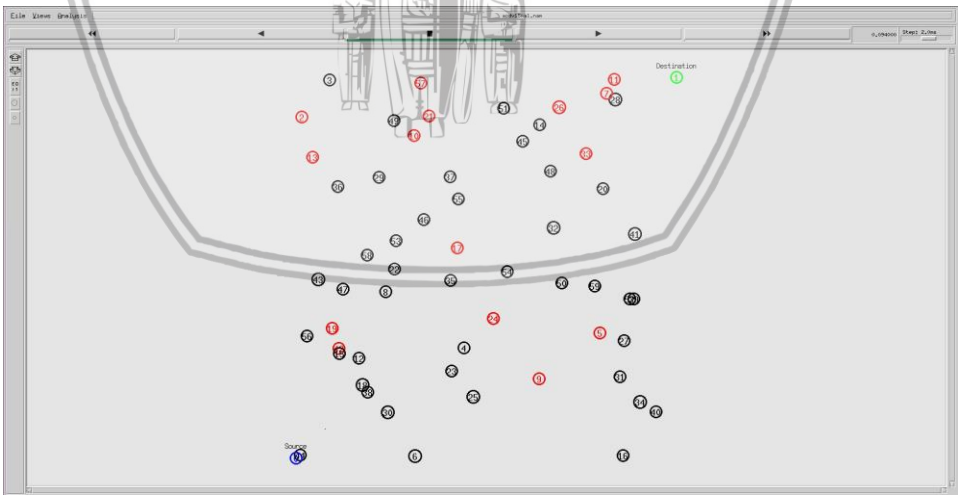
Gambar 4.10 merupakan simulasi dari topologi jaringan dengan jumlah *node* sebanyak 60 dengan variasi 5 *node black hole. Node* 0 yang berwarna biru ditetapkan sebagai *node* sumber dan *node* 1 yang berwarna hijau ditetapkan sebagai *node* tujuan. *Node-node* yang berwarna hitam merupakan *Node-node* yang akan dilewatkan paket dari sumber ke tujuan. *Node* sumber dan *node* tujuan

diletakkan saling berjauhan agar dapat memaksimalkan pengujian yang akan dilakukan.



Gambar 4.7 Topologi Jaringan 60 *node* dengan varaiasi 10 *node Black Hole*

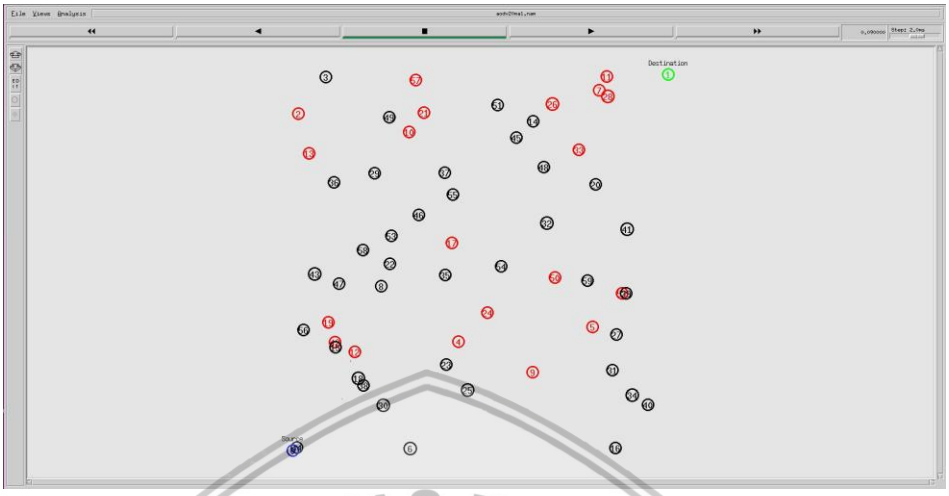
Gambar 4.11 merupakan simulasi dari topologi jaringan dengan jumlah *node* sebanyak 60 dengan variasi 10 *node black hole. Node* 0 yang berwarna biru ditetapkan sebagai *node* sumber dan *node* 1 yang berwarna hijau ditetapkan sebagai *node* tujuan. *Node-node* yang berwarna hitam merupakan *Node-node* yang akan dilewatkan paket dari sumber ke tujuan. *Node* sumber dan *node* tujuan diletakkan saling berjauhan agar dapat memaksimalkan pengujian yang akan dilakukan.



Gambar 4.8 Topologi Jaringan 60 *node* dengan variasi 15 *node Black Hole*

Gambar 4.12 merupakan simulasi dari topologi jaringan dengan jumlah *node* sebanyak 60 dengan variasi 15 *node black hole. Node* 0 yang berwarna biru ditetapkan sebagai *node* sumber dan *node* 1 yang berwarna hijau ditetapkan sebagai *node* tujuan. *Node-node* yang berwarna hitam merupakan *Node-node* yang akan dilewatkan paket dari sumber ke tujuan. *Node* sumber dan *node* tujuan

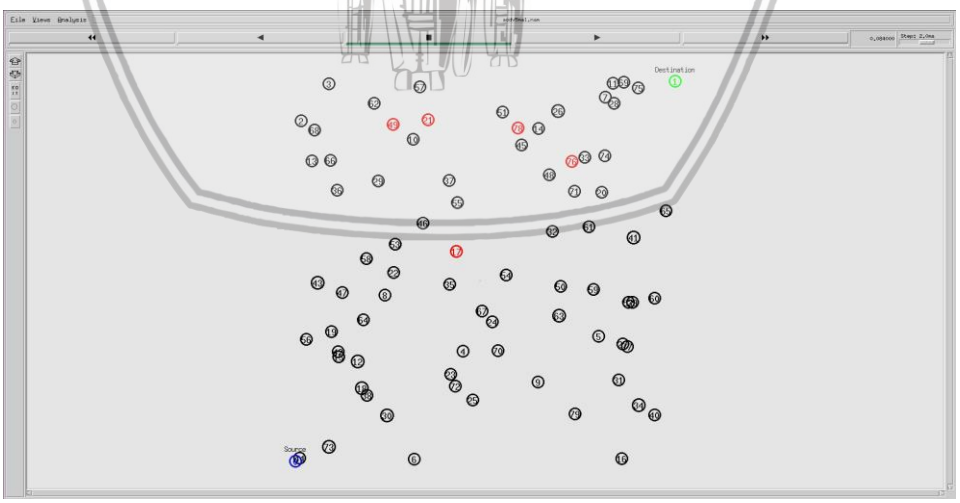
diletakkan saling berjauhan agar dapat memaksimalkan pengujian yang akan dilakukan.



Gambar 4.9 Topologi Jaringan 60 *node* dengan variasi 20 *node Black Hole*

Gambar 4.13 merupakan simulasi dari topologi jaringan dengan jumlah *node* sebanyak 60 dengan variasi 20 *node black hole. Node* 0 yang berwarna biru ditetapkan sebagai *node* sumber dan *node* 1 yang berwarna hijau ditetapkan sebagai *node* tujuan. *Node-node* yang berwarna hitam merupakan *Node-node* yang akan dilewatkan paket dari sumber ke tujuan. *Node* sumber dan *node* tujuan diletakkan saling berjauhan agar dapat memaksimalkan pengujian yang akan dilakukan.

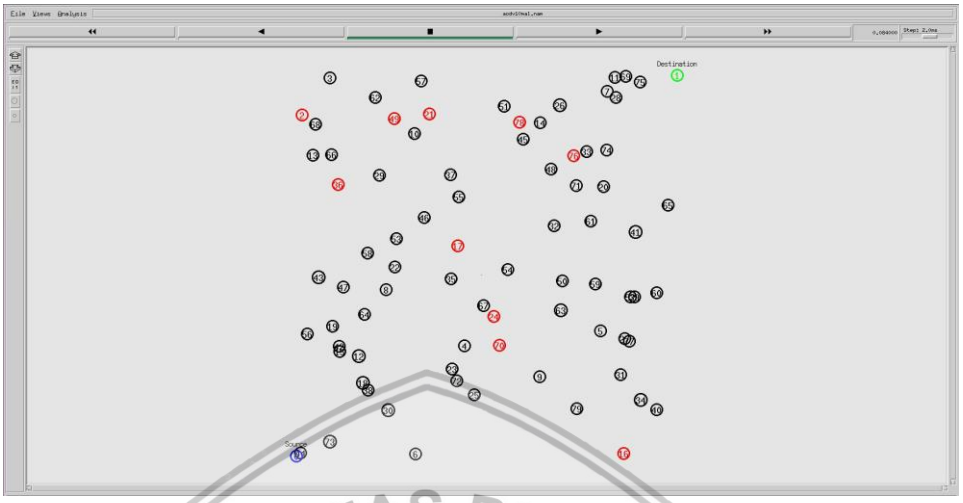
3. Topologi Jaringan 80 *node* dengan Serangan *Black Hole*



Gambar 4.10 Topologi Jaringan 80 *node* dengan variasi 5 *node Black Hole*

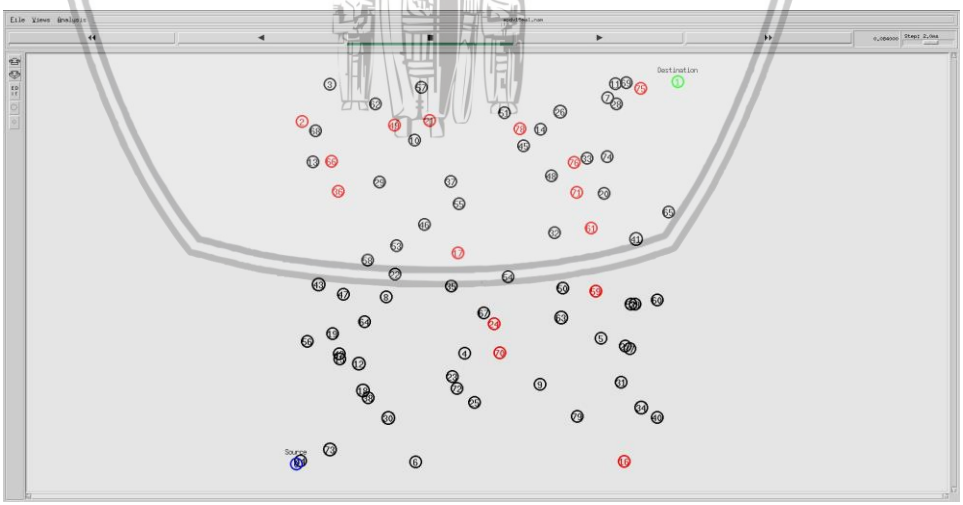
Gambar 4.14 merupakan simulasi dari topologi jaringan dengan jumlah *node* sebanyak 80 dengan variasi 5 *node black hole. Node* 0 yang berwarna biru ditetapkan sebagai *node* sumber dan *node* 1 yang berwarna hijau ditetapkan sebagai *node* tujuan. *Node-node* yang berwarna hitam merupakan *Node-node* yang akan dilewatkan paket dari sumber ke tujuan. *Node* sumber dan *node* tujuan

diletakkan saling berjauhan agar dapat memaksimalkan pengujian yang akan dilakukan.



Gambar 4.11 Topologi Jaringan 80 *node* dengan varaiasi 10 *node Black Hole*

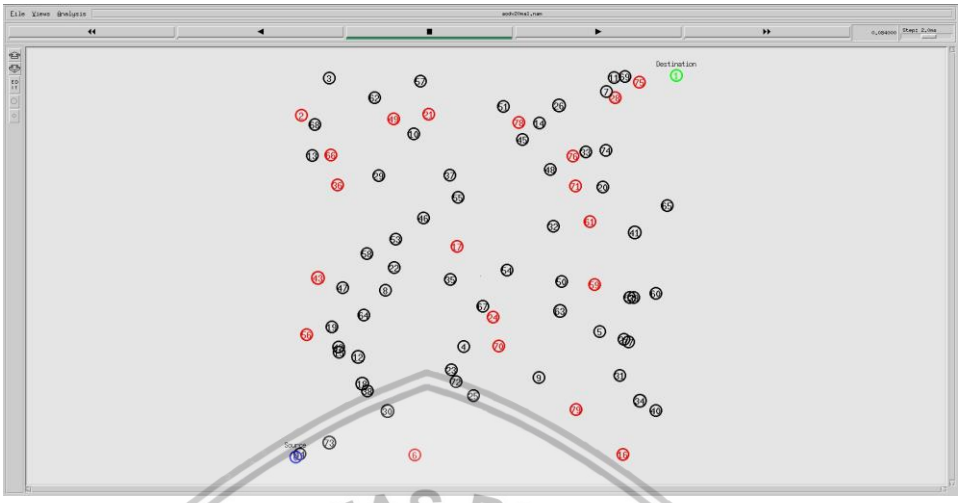
Gambar 4.15 merupakan simulasi dari topologi jaringan dengan jumlah *node* sebanyak 80 dengan variasi 10 *node black hole. Node* 0 yang berwarna biru ditetapkan sebagai *node* sumber dan *node* 1 yang berwarna hijau ditetapkan sebagai *node* tujuan. *Node-node* yang berwarna hitam merupakan *Node-node* yang akan dilewatkan paket dari sumber ke tujuan. *Node* sumber dan *node* tujuan diletakkan saling berjauhan agar dapat memaksimalkan pengujian yang akan dilakukan.



Gambar 4.12 Topologi Jaringan 80 *node* dengan variasi 15 *node Black Hole*

Gambar 4.16 merupakan simulasi dari topologi jaringan dengan jumlah *node* sebanyak 80 dengan variasi 15 *node black hole. Node* 0 yang berwarna biru ditetapkan sebagai *node* sumber dan *node* 1 yang berwarna hijau ditetapkan sebagai *node* tujuan. *Node-node* yang berwarna hitam merupakan *Node-node* yang akan dilewatkan paket dari sumber ke tujuan. *Node* sumber dan *node* tujuan

diletakkan saling berjauhan agar dapat memaksimalkan pengujian yang akan dilakukan.



Gambar 4.13 Topologi Jaringan 80 *node* dengan variasi 20 *node Black Hole*

Gambar 4.17 merupakan simulasi dari topologi jaringan dengan jumlah *node* sebanyak 80 dengan variasi 20 *node black hole. Node* 0 yang berwarna biru ditetapkan sebagai *node* sumber dan *node* 1 yang berwarna hijau ditetapkan sebagai *node* tujuan. *Node-node* yang berwarna hitam merupakan *Node-node* yang akan dilewatkan paket dari sumber ke tujuan. *Node* sumber dan *node* tujuan diletakkan saling berjauhan agar dapat memaksimalkan pengujian yang akan dilakukan.

BAB 5 PENGUJIAN DAN ANALISIS

5.1 Pengujian

Tahap ini akan dilakukan pengujian terhadap protokol AODV dan protokol DYMO. Pengujian dilakukan dengan menggunakan variasi serangan *black hole* guna menguji parameter kinerja yakni *packet delivery ratio*, *normalized routing load,* dan *packet loss*. Terdapat 3 skenario pengujian yaitu pengujian kepadatan 40 *node* dengan jumlah serangan *black hole* sebanyak 5, 10, 15, dan 20. Pengujian kepadatan 60 *node* dengan jumlah serangan *black hole* sebanyak 5, 10, 15, dan 20. Pengujian kepadatan 80 *node* dengan jumlah serangan *black hole* sebanyak 5, 10, 15, dan 20. Berikut merupakan skenario pengujian ditunjukan pada tabel 5.1.

Tabel 5.1 Tabel Skenario Pengujian

Skenario	Jumlah *Node*	Jumlah Serangan *Black Hole*
1	40	5, 10, 15, 20
2	60	5, 10, 15, 20
3	80	5, 10, 15, 20

5.1.1 Skenario Kepadatan 40 *Node*

Pada skenario kepadatan *node* 40 guna menguji parameter kinerja pada protokol AODV dan protokol DYMO yakni *packet delivery ratio*, *normalized routing laod,* dan *packet loss*.

5.1.1.1 *Packet Delivery Ratio*

Tabel 5.2 *Packet Delivery Ratio* kepadatan 40 *node*

Jumlah *Black Hole*	*Packet Delivery Ratio* (%)	
	AODV 40 *node*	DYMO 40 *node*
5 *node Black Hole*	36,9	42,8
10 *node Black Hole*	19,5	24,6
15 *node Black Hole*	14,3	21
20 *node Black Hole*	9,9	18,8

Tabel 5.2 menunjukan hasil pengujian *Packet Delivery Ratio* (PDR) pada protokol AODV dan protokol DYMO dengan kepadatan 40 *node* dan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, 20. Pengujian ini dilakukan guna

mengetahui persentase paket yang diterima pada *node* tujuan yang akan dibandingkan serta melakukan analisis pada kepadatan *node* yang lain. Pengujian PDR dilakukan menggunakan parameter simulasi yang telah ditentukan sebelumnya dan membuat algoritma sesuai dengan rumus PDR tersebut, lalu dijalankan dengan fungsi `awk -f [PDR.awk] [40node.tr]`.

Pengujian PDR pada skenario kepadatan 40 *node* diperoleh dengan hasil protokol DYMO lebih baik dibandingkan protokol AODV pada setiap variasi *node* penyerang (*black hole*). Hal ini disebabkan protokol DYMO memiliki fitur yang tidak dimiliki protokol AODV yaitu fitur *path accumulation*, yang dapat membuat protokol DYMO dapat bekerja lebih baik dalam mengatasi *route maintenance.* Pada hasil protokol AODV dan protokol DYMO akan mengalami penurunan hasil seiring bertambahnya *node black hole.* Hal ini dapat terjadi karena *node black hole* akan bersifat selayaknya *node* biasa sehingga paket yang akan melewati *node black hole* untuk ke tujuan akan di *drop* oleh *node black hole* tersebut.

5.1.1.2 *Normalized Routing Load*

Tabel 5.3 *Normalized Routing Load* kepadatan *node* 40

Jumlah *Black Hole*	*Normalized Routing Load*	
	AODV 40 *node*	DYMO 40 *node*
5 *node Black Hole*	2,02439	3,43692
10 *node Black Hole*	4,02051	4,63415
15 *node Black Hole*	5,16084	5,21905
20 *node Black Hole*	7,0303	7,39362

Tabel 5.3 menunjukan Normalize *Routing* Load (NRL) pada protokol AODV dan protokol DYMO dengan kepadatan 40 *node* dan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, 20. Pengujian ini dilakukan guna mengetahui jumlah paket *routing* kedua protokol yang dihasilkan selama simulasi dan akan dibandingkan serta melakukan analisis pada kepadatan *node* yang lain. Pengujian NRL dilakukan menggunakan parameter simulasi yang telah ditentukan sebelumnya dan membuat algoritma sesuai dengan rumus NRL tersebut, lalu dijalankan dengan fungsi `awk -f [NRL.awk] [40node.tr]`.

Pengujian NRL pada skenario kepadatan 40 *node* diperoleh dengan hasil protokol DYMO lebih besar dibandingkan protokol AODV pada semua variasi serangan *black hole.* Hal ini terjadi karena pada protokol DYMO terdapat fitur *path accumulation* yang dapat mengetahui informasi tentang semua *node* antara *node* sumber dan *node* tujuan. Sedangkan protokol AODV hanya mengetahui informasi *node* sumber dan *node* tujuan. Pada hasil protokol AODV dan protokol DYMO

mengalami kenaikan seiring bertambahnya *node black hole.* Hal ini disebabkan oleh *node black hole* yang semakin bertambah maka sehingga membuat rute ke tujuan sering terputus dan mengharuskan kedua protokol melakukan pencarian rute kembali.

5.1.1.3 *Packet Loss*

Tabel 5.4 *Packet Loss* kepadatan 40 *node*

Jumlah *Black Hole*	*Packet Loss* (%)	
	AODV 40 *node*	DYMO 40 *node*
5 *node Black Hole*	47,8	37,7
10 *node Black Hole*	64,9	57,2
15 *node Black Hole*	70,1	61,2
20 *node Black Hole*	74,5	61,9

Tabel 5.4 menunjukan *Packet Loss* pada protokol AODV dan protokol DYMO dengan kepadatan 40 *node* dan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, 20 Pengujian ini dilakukan guna mengetahui paket data yang hilang disebabkan oleh *black hole* dan akan dibandingkan serta melakukan analisis pada kepadatan *node* yang lain. Pengujian *packet loss* dilakukan menggunakan parameter simulasi yang telah ditentukan sebelumnya dan membuat algoritma sesuai dengan rumus *packet loss* tersebut, lalu dijalankan dengan fungsi `awk -f [PLBhole.awk] [40node.tr]`.

Pengujian *packet loss* pada skenario kepadatan 40 *node* diperoleh dengan hasil protokol DYMO lebih baik dibandingkan protokol AODV jika terdapat *node black hole* sedangkan protokol AODV lebih baik dibandingkan protokol DYMO jika tanpa *node black hole.* Hal ini disebabkan protokol DYMO memiliki fitur yang tidak dimiliki protokol AODV yaitu fitur *path accumulation*, yang dapat membuat protokol DYMO dapat bekerja lebih baik dalam mengatasi *route maintenance*. Pada hasil protokol AODV dan protokol DYMO, *packet loss* akan meningkat seiring bertambahnya *node black hole.* Hal ini dapat terjadi karena *node black hole* akan bersifat selayaknya *node* biasa sehingga paket yang akan melewati *node black hole* untuk ke tujuan akan di *drop* oleh *node black hole* dan menyebabkan paket tersebut hilang.

5.1.2 Skenario Kepadatan 60 *Node*

Pada skenario kepadatan *node* 60 guna menguji parameter kinerja pada protokol AODV dan protokol DYMO yakni *packet delivery ratio*, *normalized routing laod,* dan *packet loss*.

5.1.2.1 *Packet Delivery Ratio*

Tabel 5.5 *Packet Delivery Ratio* kepadatan 60 *node*

Jumlah *Black Hole*	*Packet Delivery Ratio* (%)	
	AODV 60 *node*	DYMO 60 *node*
5 *node Black Hole*	49,9	57,7
10 *node Black Hole*	37,3	50,6
15 *node Black Hole*	21,7	33,6
20 *node Black Hole*	16,4	19,6

Tabel 5.5 menunjukan hasil pengujian *Packet Delivery Ratio* (PDR) pada protokol AODV dan protokol DYMO dengan kepadatan 60 *node* dan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, 20. Pengujian ini dilakukan guna mengetahui persentase paket yang diterima pada *node* tujuan yang akan dibandingkan serta melakukan analisis pada kepadatan *node* yang lain. Pengujian PDR dilakukan menggunakan parameter simulasi yang telah ditentukan sebelumnya dan membuat algoritma sesuai dengan rumus PDR tersebut, lalu dijalankan dengan fungsi `awk -f [PDR.awk] [60node.tr]`.

Pengujian PDR pada skenario kepadatan 60 *node* diperoleh dengan hasil protokol DYMO lebih baik dibandingkan protokol AODV pada setiap variasi *node* penyerang (*black hole*). Hal ini disebabkan protokol DYMO memiliki fitur yang tidak dimiliki protokol AODV yaitu fitur *path accumulation*, yang dapat membuat protokol DYMO dapat bekerja lebih baik dalam mengatasi *route maintenance.* Pada hasil protokol AODV dan protokol DYMO akan mengalami penurunan hasil seiring bertambahnya *node black hole.* Hal ini dapat terjadi karena *node black hole* akan bersifat selayaknya *node* biasa sehingga paket yang akan melewati *node black hole* untuk ke tujuan akan di *drop* oleh *node black hole* tersebut.

5.1.2.2 *Normalized Routing Load*

Tabel 5.6 *Normalized Routing Load* kepadatan 60 *node*

Jumlah *Black Hole*	*Normalized Routing Load*	
	AODV 60 *node*	DYMO 60 *node*
5 *node Black Hole*	2,46493	4,55113
10 *node Black Hole*	4,18231	5,08103

15 *node Black Hole*	5,95853	6,05357
20 *node Black Hole*	7,7561	7,90816

Tabel 5.6 menunjukan Normalize *Routing* Load (NRL) pada protokol AODV dan protokol DYMO dengan kepadatan 60 *node* dan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, 20. Pengujian ini dilakukan guna mengetahui jumlah paket *routing* kedua protokol yang dihasilkan selama simulasi dan akan dibandingkan serta melakukan analisis pada kepadatan *node* yang lain. Pengujian NRL dilakukan menggunakan parameter simulasi yang telah ditentukan sebelumnya dan membuat algoritma sesuai dengan rumus NRL tersebut, lalu dijalankan dengan fungsi `awk -f [NRL.awk] [60node.tr]`.

Pengujian NRL pada skenario kepadatan 60 *node* diperoleh dengan hasil protokol DYMO lebih besar dibandingkan protokol AODV pada semua variasi serangan *black hole.* Hal ini terjadi karena pada protokol DYMO terdapat fitur *path accumulation* yang dapat mengetahui informasi tentang semua *node* antara *node* sumber dan *node* tujuan. Sedangkan protokol AODV hanya mengetahui informasi *node* sumber dan *node* tujuan. Pada hasil protokol AODV dan protokol DYMO mengalami kenaikan seiring bertambahnya *node black hole.* Hal ini disebabkan oleh *node black hole* yang semakin bertambah maka sehingga membuat rute ke tujuan sering terputus dan mengharuskan kedua protokol melakukan pencarian rute kembali.

5.1.2.3 *Packet Loss*

Tabel 5.7 *Packet Loss* kepadatan 60 *node*

Jumlah *Black Hole*	*Packet Loss* (%)	
	AODV 60 *node*	DYMO 60 *node*
5 *node Black Hole*	37,7	24,8
10 *node Black Hole*	49,8	32,4
15 *node Black Hole*	65,9	50,7
20 *node Black Hole*	70,9	61

Tabel 5.7 menunjukan *Packet Loss* pada protokol AODV dan protokol DYMO dengan kepadatan 60 *node* dan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, 20 Pengujian ini dilakukan guna mengetahui paket data yang hilang disebabkan oleh *black hole* dan akan dibandingkan serta melakukan analisis

pada kepadatan *node* yang lain. Pengujian *packet loss* dilakukan menggunakan parameter simulasi yang telah ditentukan sebelumnya dan membuat algoritma sesuai dengan rumus *packet loss* tersebut, lalu dijalankan dengan fungsi `awk -f [PLBhole.awk] [60node.tr]`.

Pengujian *packet loss* pada skenario kepadatan 60 *node* diperoleh dengan hasil protokol DYMO lebih baik dibandingkan protokol AODV jika terdapat *node black hole* sedangkan protokol AODV lebih baik dibandingkan protokol DYMO jika tanpa *node black hole.* Hal ini disebabkan protokol DYMO memiliki fitur yang tidak dimiliki protokol AODV yaitu fitur *path accumulation*, yang dapat membuat protokol DYMO dapat bekerja lebih baik dalam mengatasi *route maintenance*. Pada hasil protokol AODV dan protokol DYMO, *packet loss* akan meningkat seiring bertambahnya *node black hole.* Hal ini dapat terjadi karena *node black hole* akan bersifat selayaknya *node* biasa sehingga paket yang akan melewati *node black hole* untuk ke tujuan akan di *drop* oleh *node black hole* dan menyebabkan paket tersebut hilang.

5.1.3 Skenario Kepadatan 80 *Node*

Pada skenario kepadatan *node* 80 guna menguji parameter kinerja pada protokol AODV dan protokol DYMO yakni *packet delivery ratio*, *normalized routing laod,* dan *packet loss*.

5.1.3.1 *Packet Delivery Ratio*

Tabel 5.8 *Packet Delivery Ratio* kepadatan 80 *node*

Jumlah *Black Hole*	*Packet Delivery Ratio* (%)	
	AODV 80 *node*	DYMO 80 *node*
5 *node Black Hole*	74,1	77,1
10 *node Black Hole*	50,9	66,1
15 *node Black Hole*	43,6	54,6
20 *node Black Hole*	35,9	38,7

Tabel 5.8 menunjukan hasil pengujian *Packet Delivery Ratio* (PDR) pada protokol AODV dan protokol DYMO dengan kepadatan 80 *node* dan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, 20. Pengujian ini dilakukan guna mengetahui persentase paket yang diterima pada *node* tujuan yang akan dibandingkan serta melakukan analisis pada kepadatan *node* yang lain. Pengujian PDR dilakukan menggunakan parameter simulasi yang telah ditentukan sebelumnya dan membuat algoritma sesuai dengan rumus PDR tersebut, lalu dijalankan dengan fungsi `awk -f [PDR.awk] [80node.tr]`.

Pengujian PDR pada skenario kepadatan 80 *node* diperoleh dengan hasil protokol DYMO lebih baik dibandingkan protokol AODV pada setiap variasi *node* penyerang (*black hole*). Hal ini disebabkan protokol DYMO memiliki fitur yang tidak dimiliki protokol AODV yaitu fitur *path accumulation*, yang dapat membuat protokol DYMO dapat bekerja lebih baik dalam mengatasi *route maintenance.* Pada hasil protokol AODV dan protokol DYMO akan mengalami penurunan hasil seiring bertambahnya *node black hole.* Hal ini dapat terjadi karena *node black hole* akan bersifat selayaknya *node* biasa sehingga paket yang akan melewati *node black hole* untuk ke tujuan akan di *drop* oleh *node black hole* tersebut.

5.1.3.2 *Normalized Routing Load*

Tabel 5.9 *Normalized Routing Load* kepadatan 80 *node*

Jumlah *Black Hole*	*Normalized Routing Load*	
	AODV 80 *node*	DYMO 80 *node*
5 *node Black Hole*	3,97976	5,81193
10 *node Black Hole*	4,35953	6,00454
15 *node Black Hole*	6,07339	7,22711
20 *node Black Hole*	7,92479	8,18346

Tabel 5.9 menunjukan Normalize *Routing* Load (NRL) pada protokol AODV dan protokol DYMO dengan kepadatan 80 *node* dan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, 20. Pengujian ini dilakukan guna mengetahui jumlah paket *routing* kedua protokol yang dihasilkan selama simulasi dan akan dibandingkan serta melakukan analisis pada kepadatan *node* yang lain. Pengujian NRL dilakukan menggunakan parameter simulasi yang telah ditentukan sebelumnya dan membuat algoritma sesuai dengan rumus NRL tersebut, lalu dijalankan dengan fungsi `awk -f [NRL.awk] [80node.tr]`.

Pengujian NRL pada skenario kepadatan 80 *node* diperoleh dengan hasil protokol DYMO lebih besar dibandingkan protokol AODV pada semua variasi serangan *black hole.* Hal ini terjadi karena pada protokol DYMO terdapat fitur *path accumulation* yang dapat mengetahui informasi tentang semua *node* antara *node* sumber dan *node* tujuan. Sedangkan protokol AODV hanya mengetahui informasi *node* sumber dan *node* tujuan. Pada hasil protokol AODV dan protokol DYMO mengalami kenaikan seiring bertambahnya *node black hole.* Hal ini disebabkan oleh *node black hole* yang semakin bertambah maka sehingga membuat rute ke tujuan sering terputus dan mengharuskan kedua protokol melakukan pencarian rute kembali.

5.1.3.3 *Packet Loss*

Tabel 5.10 *Packet Loss* kepadatan 80 *node*

Jumlah *Black Hole*	*Packet Loss* (%)	
	AODV 80 *node*	DYMO 80 *node*
5 *node Black Hole*	24,2	16,7
10 *node Black Hole*	47,9	28,3
15 *node Black Hole*	54,8	39,7
20 *node Black Hole*	62,6	57,1

Tabel 5.10 menunjukan *Packet Loss* pada protokol AODV dan protokol DYMO dengan kepadatan 80 *node* dan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, 20 Pengujian ini dilakukan guna mengetahui paket data yang hilang disebabkan oleh *black hole* dan akan dibandingkan serta melakukan analisis pada kepadatan *node* yang lain. Pengujian *packet loss* dilakukan menggunakan parameter simulasi yang telah ditentukan sebelumnya dan membuat algoritma sesuai dengan rumus *packet loss* tersebut, lalu dijalankan dengan fungsi `awk -f [PLBhole.awk] [80node.tr]`.

Pengujian *packet loss* pada skenario kepadatan 80 *node* diperoleh dengan hasil protokol DYMO lebih baik dibandingkan protokol AODV jika terdapat *node black hole* sedangkan protokol AODV lebih baik dibandingkan protokol DYMO jika tanpa *node black hole.* Hal ini disebabkan protokol DYMO memiliki fitur yang tidak dimiliki protokol AODV yaitu fitur *path accumulation*, yang dapat membuat protokol DYMO dapat bekerja lebih baik dalam mengatasi *route maintenance*. Pada hasil protokol AODV dan protokol DYMO, *packet loss* akan meningkat seiring bertambahnya *node black hole.* Hal ini dapat terjadi karena *node black hole* akan bersifat selayaknya *node* biasa sehingga paket yang akan melewati *node black hole* untuk ke tujuan akan di *drop* oleh *node black hole* dan menyebabkan paket tersebut hilang.

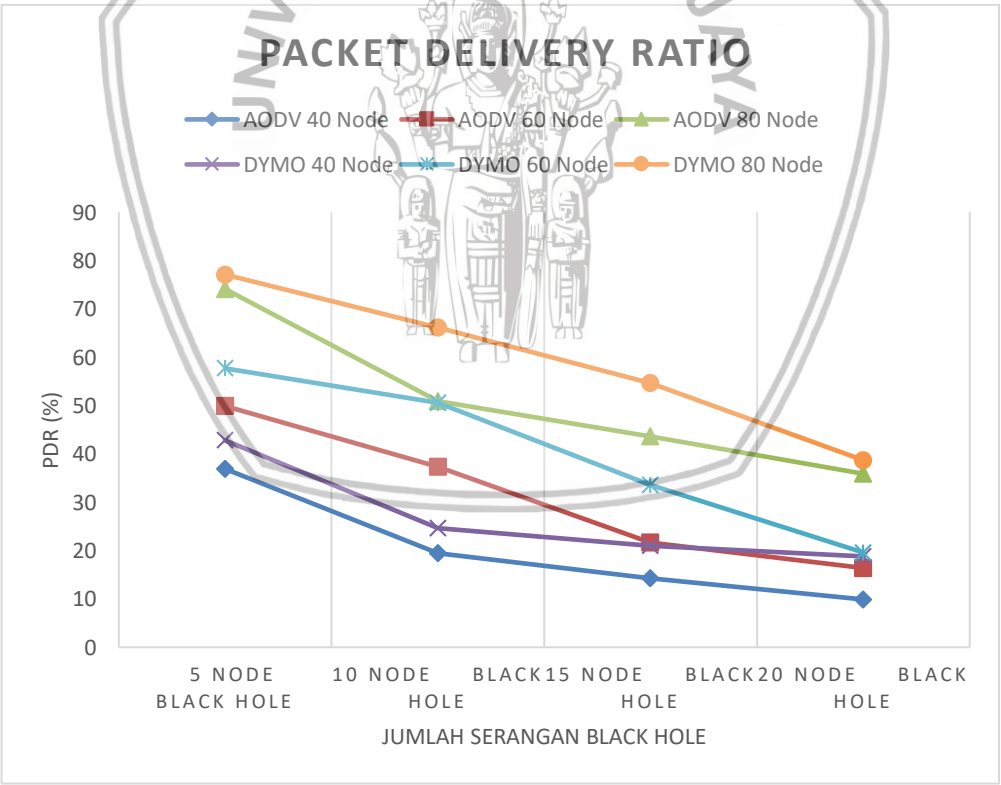
5.2 Analisis

Tahap ini akan dilakukan analisis terhadap hasil yang diperoleh pada semua skenario pengujian. Analisis dilakukan terhadap hasil pengujian kepadatan jumlah *node* 40, 60, 80 dengan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, dan 20 yang diukur menggunakan parameter kinerja *packet delivery ratio*, *normalized routing load,* dan *packet loss*.

5.2.1 *Packet Delivery Ratio*

Tabel 5.11 Hasil Parameter Pengujian *Packet Delivery Ratio*

Jumlah *Black Hole*	*Packet Delivery Ratio* (%)					
	AODV 40 *node*	AODV 60 *node*	AODV 80 *node*	DYMO 40 *node*	DYMO 60 *node*	DYMO 80 *node*
5 *node Black Hole*	36,9	49,9	74,1	42,8	57,7	77,1
10 *node Black Hole*	19,5	37,3	50,9	24,6	50,6	66,1
15 *node Black Hole*	14,3	21,7	43,6	21	33,6	54,6
20 *node Black Hole*	9,9	16,4	35,9	18,8	19,6	38,7



Gambar 5.1 Hasil Parameter Pengujian *Packet Delivery Ratio*

Gambar 5.1 menunjukan *Packet Delivery Ratio* (PDR) pada protokol AODV dan protokol DYMO dengan skenario jumlah kepadatan *node* sebanyak 40, 60, 80 *node* dan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, 20. Secara

umum hasil pengujian pada parameter *packet delivery ratio* menunjukan penurunan seiring bertambahnya *node black hole* karena *node black hole* akan bersifat selayaknya *node* biasa sehingga seiring bertambahnya *node black hole* maka paket akan lebih sering di *drop* karena kemungkinan melewatkan *node black hole* akan bertambah pula.

Pada hasil skenario pengujian kepadatan *node* 40, 60, dan 80 akan mengalami kenaikan persentase pada setiap skenarionya, baik protokol AODV maupun protokol DYMO. Dapat ditunjukan pada gambar 5.1, dimana protokol AODV dan protokol DYMO pada kepadatan *node* 80 akan mendapatkan hasil lebih besar dibandingkan kepadatan *node* 60 dan kepadatan *node* 60 akan mendapat hasil lebih besar dibandingkan kepadatan *node* 40. Hal ini dapat terjadi karena semakin padat *node* pada sebuah area akan memudahkan *node-node* tersebut mencari jalur dari sumber ke tujuan sehingga akan membuat persentase meningkat seiring bertambahnya kepadatan *node*. Pada hasil pengujian protokol DYMO dengan semua kepadatan jumlah *node* mendapatkan hasil PDR lebih baik dibandingkan dengan protokol AODV dengan semua variasi jumlah *node* penyerang (*black hole*) sehingga protokol DYMO dapat dikatakan lebih baik dibandingkan protokol AODV saat terdapat *node black hole* pada semua kepadatan jumlah *node*. Hal dapat terjadi karena protokol DYMO memiliki fitur yang tidak dimiliki AODV yaitu fitur *path accumulation*, dimana fitur tersebut membantu protokol DYMO menemukan jalur baru ke tujuan saat rute terputus.

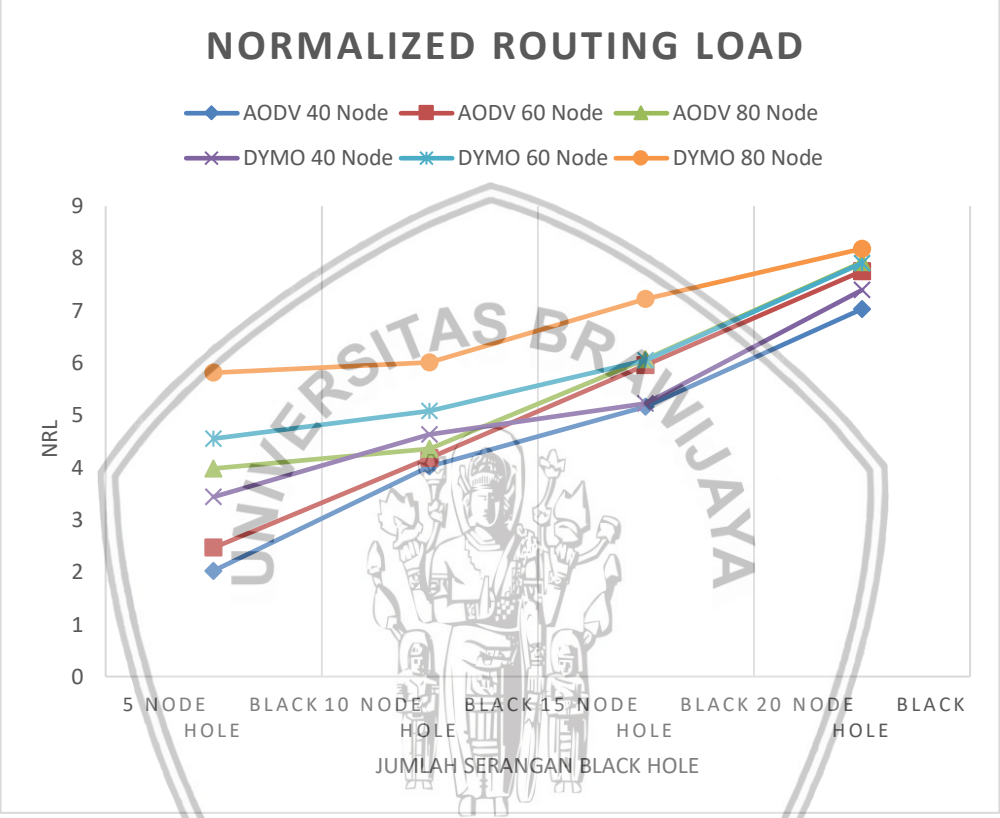
Hasil pengujian pada parameter *packet delivery ratio* mendapatkan hasil protokol DYMO lebih baik dibandingkan protokol AODV. Diperoleh rata-rata keseluruhan hasil PDR pada protokol AODV sebesar 34,2%. Sedangkan pada protokol DYMO sebesar 42,1%. Pada hasil rata-rata setiap *node black hole* diperoleh PDR pada protokol AODV sebesar 53,6% untuk 5 *node black hole,* 35,9% untuk 10 *node black hole,* 26,5% untuk 15 *node black hole,* dan 20,7% untuk 20 *node black hole*. Sedangkan pada protokol DYMO sebesar 59,2% untuk 5 *node black hole,* 47,1% untuk 10 *node black hole,* 36,4% untuk 15 *node black hole,* dan 25,7% untuk 20 *node black hole.* Pada saat ditambahkan serangan *black hole,* hasil PDR pada protokol AODV dan protokol DYMO akan mengalami penurunan. Sehingga dapat disimpulkan bahwa serangan *black hole* dapat mempengaruhi kinerja kedua protokol dalam proses pengiriman paket ke tujuan.

5.2.2 *Normalized Routing Load*

Tabel 5.12 Hasil Parameter Pengujian *Normalized Routing Load*

Jumlah *Black Hole*	*Normalized Routing Load*					
	AODV 40 *node*	AODV 60 *node*	AODV 80 *node*	DYMO 40 *node*	DYMO 60 *node*	DYMO 80 *node*
5 *node Black Hole*	2,02439	2,46493	3,97976	3,43692	4,55113	5,81193

10 *node Black Hole*	4,02051	4,18231	4,35953	4,63415	5,08103	6,00454
15 *node Black Hole*	5,16084	5,95853	6,07339	5,21905	6,05357	7,22711
20 *node Black Hole*	7,0303	7,7561	7,92479	7,39362	7,90816	8,18346



Gambar 5.2 Hasil Parameter Pengujian *Normalized Routing Load*

Gambar 5.2 menunjukan *Normalized Routing Load* (NRL) pada protokol AODV dan protokol DYMO dengan skenario jumlah kepadatan *node* sebanyak 40, 60, 80 *node* dan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, 20. Secara umum hasil pengujian pada parameter *normalized routing* load menunjukan kenaikan pada hasil pengujian seiring bertambahnya *node black hole.* Hal ini dapat terjadi karena seiring bertambahnya *node black hole* akan membuat paket data yang sampai tujuan akan berkurang. Dilihat dari rumus NRL yaitu total paket *routing* yang dikirim dibagi total paket data yang diterima tujuan, sehingga pembagi semakin kecil akan mendapatkan hasil NRL semakin besar.

Pada hasil skenario pengujian kepadatan *node* 40, 60, dan 80 akan mengalami kenaikan pada setiap skenarionya, baik protokol AODV maupun DYMO. Dapat ditunjukan pada gambar 5.2, dimana protokol AODV dan protokol DYMO pada kepadatan *node* 80 akan mendapatkan hasil lebih besar dibandingkan kepadatan *node* 60 dan kepadatan *node* 60 akan mendapat hasil lebih besar dibandingkan kepadatan *node* 40. Hal ini terjadi karena semakin padat *node* pada

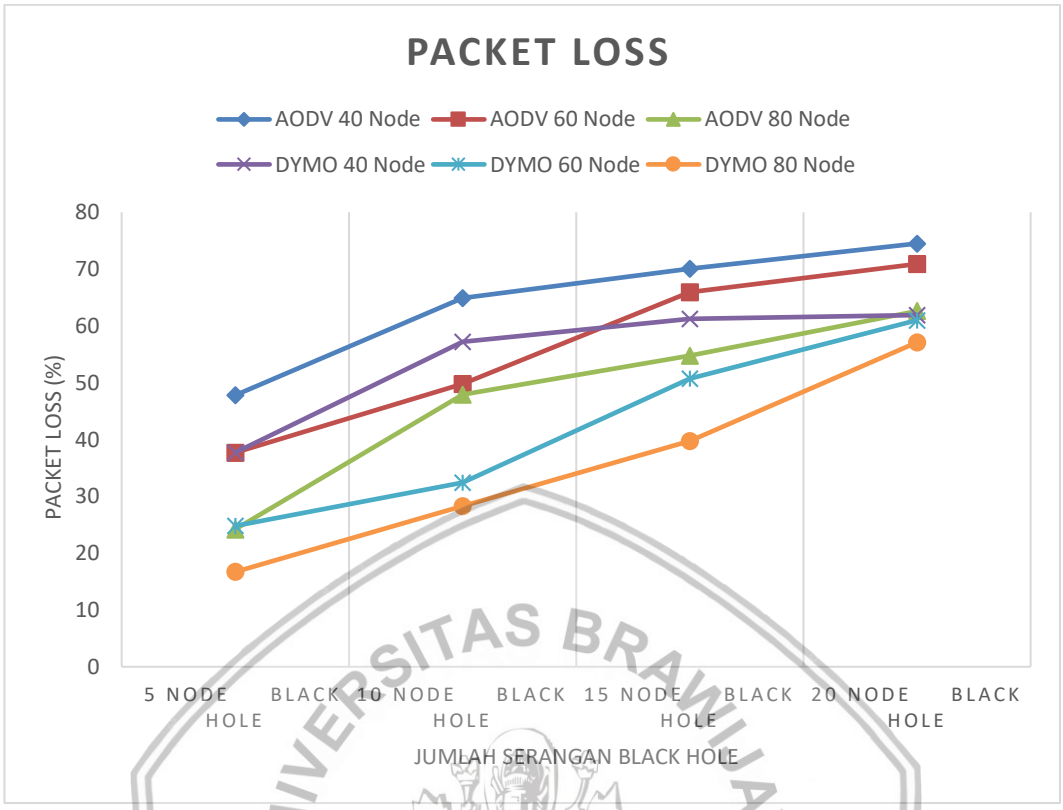
sebuah area maka akan lebih banyak *node* yang saling bertukar pesan untuk mendapatkan jalur ketujuan. Nilai NRL pada protokol DYMO cukup besar dibandingkan pada protokol AODV pada setiap kepadatan jumlah *node*. Hal ini terjadi karena pada fitur *path accumulation* protokol DYMO melakukan pengiriman RREQ terhadap semua opsi tetangga terdekat memiliki jalur ke tujuan dan tetangga yang menerima pesan RREQ akan mengirimkan kembali pesan RREQ ke semua opsi tetangga terdekat *node* tersebut hingga mencapai tujuan. Sedangkan protokol AODV hanya melakukan pengiriman RREQ terhadap tetangga terdekat hingga mencapai tujuan.

Hasil pengujian pada parameter *normalized routing load* mendapatkan hasil protokol AODV lebih baik dibandingkan protokol DYMO. Diperoleh rata-rata keseluruhan hasil NRL pada protokol AODV sebesar 5,0779. Sedangkan pada protokol DYMO sebesar 5,9587. Pada hasil rata-rata setiap *node black hole* diperoleh NRL pada protokol AODV sebesar 2,82303 untuk 5 *node black hole,* 4,18745 untuk 10 *node black hole,* 5,73092 untuk 15 *node black hole,* dan 7,57039 untuk 20 *node black hole.* Sedangkan pada protokol DYMO sebesar 4,59999 untuk 5 *node black hole,* 5,23990 untuk 10 *node black hole,* 6,16657 untuk 15 *node black hole,* dan 7,82841 untuk 20 *node black hole.* Hasil protokol AODV relatif lebih rendah dibandingkan protokol DYMO yang menggambarkan kepadatan jaringan pada protokol AODV tidak sepadat protokol DYMO. Pada saat ditambahkan serangan *black hole* hasil akan terus meningkat pada kedua protokol, sehingga dapat disimpulkan bahwa serangan *black hole* dapat membuat jaringan semakin padat dan memyebabkan penurunan kinerja pada kedua protokol.

5.2.3 *Packet Loss*

Tabel 5.13 Parameter Hasil Pengujian *Packet Loss*

Jumlah *Black Hole*	*Packet Loss* (%)					
	AODV 40 *node*	AODV 60 *node*	AODV 80 *node*	DYMO 40 *node*	DYMO 60 *node*	DYMO 80 *node*
5 *node Black Hole*	47,8	37,7	24,2	37,7	24,8	16,7
10 *node Black Hole*	64,9	49,8	47,9	57,2	32,4	28,3
15 *node Black Hole*	70,1	65,9	54,8	61,2	50,7	39,7
20 *node Black Hole*	74,5	70,9	62,6	61,9	61	57,1



Gambar 5.3 Hasil Parameter Pengujian *Packet Loss*

Gambar 5.3 menunjukan *Packet Loss* pada protokol AODV dan protokol DYMO dengan skenario jumlah kepadatan *node* sebanyak 40, 60, 80 *node* dan variasi jumlah *node* penyerang (*black hole*) sebanyak 5, 10, 15, 20. Secara umum hasil pengujian *packet loss* menunjukan peningkatan seiring bertambahnya *node black hole* karena *node black hole* akan bersifat selayaknya *node* biasa sehingga seiring bertambahnya *node black hole* maka paket akan lebih sering di *drop* karena kemungkinan melewatkan *node black hole* akan bertambah pula dan menyebabkan packet akan hilang.

Pada hasil skenario pengujian kepadatan *node* 40, 60, dan 80 akan mengalami penurunan persentase pada setiap skenarionya, baik protokol AODV maupun protokol DYMO. Dapat ditunjukan pada gambar 5.3, dimana protokol AODV dan protokol DYMO pada kepadatan *node* 80 akan mendapatkan hasil lebih kecil dibandingkan kepadatan *node* 50 dan kepadatan *node* 50 akan mendapat hasil lebih kecil dibandingkan kepadatan *node* 30. Hal ini dapat terjadi karena semakin padat *node* pada sebuah area akan memudahkan *node-node* tersebut mencari jalur dari sumber ke tujuan sehingga akan membuat *packet loss* menurun seiring bertambahnya kepadatan *node*. Saat terdapat variasi jumlah *node* penyerang (*black hole*), protokol AODV akan menghasilkan paket loss yang lebih dibandingkan protokol DYMO pada semua variasi jumlah *node* penyerang (*black hole*) sehingga protokol DYMO dapat dikatakan lebih baik dibandingkan protokol AODV saat terdapat *node black hole* pada semua kepadatan jumlah *node*. Hal dapat terjadi karena protokol DYMO memiliki fitur yang tidak dimiliki AODV yaitu

fitur *path accumulation*, dimana fitur tersebut membantu protokol DYMO menemukan jalur baru ke tujuan saat rute terputus.

Hasil pengujian pada parameter *packet loss* mendapatkan hasil protokol DYMO lebih baik dibandingkan protokol AODV. Diperoleh rata-rata keseluruhan hasil *packet loss* pada protokol AODV sebesar 55,9%. Sedangkan pada protokol DYMO sebesar 44,1%. Pada hasil rata-rata setiap *node black hole* diperoleh *packet loss* pada protokol AODV sebesar 36,6% untuk 5 *node black hole,* 54,2% untuk 10 *node black hole,* 63,6% untuk 15 *node black hole,* dan 69,3% untuk 20 *node black hole.* Sedangkan pada protokol DYMO sebesar 26,4% untuk 5 *node black hole,* 39,3% untuk 10 *node black hole,* 50,5% untuk 15 *node black hole,* dan 60% untuk 20 *node black hole.* Pada saat ditambahkan serangan *black hole packet loss* pada protokol AODV dan protokol DYMO akan meningkat. Sehingga dapat disimpulkan bahwa serangan *black hole* dapat mempengaruhi kinerja kedua protokol hilangnya paket data yang disebabkan oleh serangan *black hole.*

BAB 6 PENUTUP

6.1 Kesimpulan

Berdasarkan hasil pengujian dan analisis dari dampak serangan *black hole* terhadap kinerja protokol AODV dan protokol DYMO pada MANET, dapat disimpulkan bahwa :

1. Implementasi serangan *black hole* pada protokol AODV dan protokol DYMO meyebabkan penurunan kinerja protokol pada parameter kinerja yang telah diujikan yaitu *packet delivery ratio*, *normalized routing load*, dan *packet loss*.
2. Kepadatan jumlah *node* dengan variasi banyak *node* penyerang (*black hole*) berpengaruh terhadap kinerja protokol AODV dan protokol DYMO. Semakin besar jumlah kepadatan *node* akan mendapatkan kinerja yang lebih baik pada parameter kinerja packet delivery ratio dan packet loss karena memudahkan *node* mencari jalur ke tujuan. Kinerja kedua protokol akan menurun pada parameter kinerja normalized routing load karena *node* yang semakin banyak akan semakin banyak pertukaran pesan antar *node*.
3. Pada parameter kinerja *packet delivery ratio* didapatkan protokol DYMO lebih baik dibandingkan AODV. Diperoleh rata-rata keseluruhan hasil PDR pada protokol AODV sebesar 34,2%. Sedangkan pada protokol DYMO sebesar 42,1%. Pada parameter kinerja *normalized routing load* didapatkan protokol AODV lebih baik dibandingkan DYMO. Diperoleh rata-rata keseluruhan hasil NRL pada protokol AODV sebesar 5,0779. Sedangkan pada protokol DYMO sebesar 5,9587. Pada parameter kinerja *packet loss* didapatkan protokol DYMO lebih baik dibandingkan AODV saat terdapat serangan *black hole.* Diperoleh rata-rata keseluruhan hasil *packet loss* pada protokol AODV sebesar 55,9%. Sedangkan pada protokol DYMO sebesar 44,1%.

6.2 Saran

Saran yang disampaikan untuk penelitian lebih lanjut adalah sebagai berikut :

1. Perlu dilakukan penelitian lebih lanjut dengan model pergerakan dan juga jumlah kepadatan *node* yang berbeda.
2. Perlu dilakukan pengujian terhadap jenis serangan malicious *node* yang berbeda seperti grayhole, sinkhole, dll.

DAFTAR REFERENSI

Agrawal, R., 2012. Performance Comparison of AODV and DYMO MANET Protocols under Wormhole Attack Environment. *International Journal of Computer Applications (0975 – 8887),* 44(9), pp. 9 - 12.

Al-Maashri, A. & Ould-Khaoua, M., 2006. Performance analysis of MANET routing protocols in the presence of self-similar traffic. *Proceedings of the 31st IEEE Conference on Local Computer Networks,* pp. 801-807.

Amillia, F., 2014. Analisis Perbandingan Kinerja Protokol Dynamic Source Routing (DSR) dan Geographic Routing Protocol (GRP) pada Mobile Ad Hoc Network (MANET). *Jurnal Sains, Teknologi dan Industri,* 12(1), pp. 9-15.

Anshori, H. A., 2013. *Analisa Perbandingan Routing Protocol DYMO dan AODV pada Vehicular Ad Hoc Network,* s.l.: Telkom University.

Ardiyansyah, F., 2016. Simulasi Serangan Black Hole pada MANET (Mobile Ad Hoc Network). *Jurnal Mahasiswa TEUB,* 4(8).

Chavan, A. A., 2016. Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack. *7th International Conference on Communication, Computing and Virtualization 2016,* pp. 835-844.

Deka, S. & Khaturia, M., 2014. Performance Analysis of DYMO Routing Protocol under Wormhole Attack in MANET. *International Journal of Science, Engineering and Technology Research (IJSETR),* 3(6), pp. 1837-1842.

Harahap, E. H., 2014. Analisis Performansi Protokol AODV (Ad Hoc On Demand Distance) dan DSR (Dynamic Source Routing) terhadap Active Attack pada MANET (Mobile Ad Hoc Network) ditinjau dari QOS (Quality Of Service) Jaringan. *e-Proceeding of Engineering,* 1(1), pp. 118-125.

Jamal, J., t.thn. *eexploria.* [Online] Available at: https://www.eexploria.com/routing-protocols-in-manets/ [Diakses 6 10 2018].

Kaur, J., 2014. Performance Analysis of AODV and DYMO Routing Protocols in MANETs Using Cuckoo Search Optimization. *International Journal of Advance Research in Computer Science and Management Studies,* 2(8), pp. 236-247.

Khetmal, M., 2013. MANET: Black Hole Node Detection in AODV. *International Journal of Computational Engineering Research,* 03(6), pp. 79-85.

Kute, V. B., 2014. Quality of Service Assessment of AOMDV for Random Waypoint and Random Walk Mobility Models. *International Journal of Computer Science and Mobile Computing,* 3(1), pp. 199-203.

Lee, F., 2011. Routing in Mobile Ad Hoc Networks. Dalam: P. X. Wang, penyunt. *Mobile Ad-Hoc Networks: Protocol Design.* USA: InTech, pp. 299-322.

Puray, M. & Palod, P., 2016. Black-Hole Attack in MANET: A Study. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* 5(3), pp. 597-601.

Rohal, P., Dahiya, R. & Dahiya, P., 2013. Study and Analysis of Throughput, Delay and Packet Delivery Ratio in MANET for Topology Based Routing Protocols (AODV, DSR and DSDV). *INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY,* 1(2), pp. 54-58.

Sakalabattula, S. K. & Kumar, S. S., 2017. Overview (Advantages and Routing Protocols) of MANET. *Advances in Computational Sciences and Technology,* 10(5), pp. 885-861.

Shukla, A., 2014. A Review on Detecting and Mitigating Techniques of Black-Hole Attack from Aodv in Manet. *International Journal of Engineering Research & Technology (IJERT),* 3(11), pp. 755-758.

Sukhija, I., 2015. A Comparative Study & Analysis of Random Waypoint and Reference Point Group Mobility Model in Ad-hoc networks. *International Journal of Advanced Research in Computer Engineering & Technology,* 4(4), pp. 1170-1172.

Wirawan, A. B., 2004. *Mudah Membangun Simulasi dengan Network Simulator-2.* Yogyakarta: Andi.